**1523213**

**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:**<br><br>**Electronic Payment Systems, LLC,** a limited liability company, d/b/a EPS,<br><br>**Electronic Payment Transfer, LLC,** a limited liability company, d/b/a EPS,<br><br>**John Dorsey,** individually and as an officer of Electronic Payment Systems, LLC and Electronic Payment Transfer, LLC, and<br><br>**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:

1. Respondent Electronic Payment Systems, LLC, also doing business as EPS, is a Colorado limited liability company with its principal office or place of business at 6472 S. Quebec St., Englewood, Colorado 80111.

2. Respondent Electronic Payment Transfer, LLC, also doing business as EPS, is a Colorado limited liability company with its principal office or place of business at 6472 S. Quebec St., Englewood, Colorado 80111.

3. Respondent John Dorsey is an owner and officer of the Proposed Corporate Respondents, Electronic Payment Systems, LLC and Electronic Payment Transfer, LLC. Individually or in concert with others, he controlled or had the authority to control, or participated in the acts and practices of Electronic Payment Systems, LLC and Electronic Payment Transfer, LLC, including the acts and practices alleged in this complaint. His principal office or place of business is the same as that of Electronic Payment Systems, LLC and Electronic Payment Transfer, LLC.

4. Respondent Thomas McCann is an owner and officer of the Proposed Corporate Respondents, Electronic Payment Systems, LLC and Electronic Payment Transfer, LLC. Individually or in concert with others, he controlled or had the authority to control, or participated in the acts and practices of Electronic Payment Systems, LLC and Electronic Payment Transfer, LLC, including the acts and practices alleged in this complaint. His principal office or place of business is the same as that of Electronic Payment Systems, LLC and Electronic Payment Transfer, LLC.

5. Respondents Electronic Payment Systems, LLC and Electronic Payment Transfer, LLC (collectively, "EPS" or "Corporate Respondents") have operated as a common enterprise while engaging in the unlawful acts and practices alleged below. Respondents have conducted the business practices described below through interrelated companies that have common ownership, officers, managers, and office locations. Because these Corporate Respondents have operated as a common enterprise, each of them is jointly and severally liable for the acts and practices alleged below. Respondents Dorsey and McCann have formulated, directed, controlled, or had the authority to control, or participated in the acts and practices of the common enterprise alleged in this complaint.

6. Respondent EPS is an independent sales organization ("ISO") that serves as an intermediary between merchants seeking to open credit card merchant accounts and its acquiring bank ("acquirer"), which is the bank that has access to the credit card networks.

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 and falsely promising that consumers would earn thousands of dollars in income.

9. The principals of the MNF scam went to great lengths to hide their identities behind a large number of phony "businesses." In order to charge consumers' credit cards but make it difficult to trace the money back to MNF, MNF engaged in a credit card laundering scheme whereby its principals and employees created numerous fictitious companies. Those fictitious companies, through a sales agent, submitted applications for merchant accounts to Respondents; Respondents then opened merchant accounts in the names of these fictitious companies, and victim credit card charges were processed through those accounts, rather than through a single merchant account in the name of MNF.

10. The practice of processing credit card transactions through another company's merchant accounts is called "credit card laundering" or "factoring" in the credit card industry. It is strictly forbidden by the credit card companies and is illegal under the Telemarketing Sales Rule ("TSR"), 16 C.F.R. Part 310.

11. The banking system behind credit card processing involves a complex series of exchanges involving numerous entities. These entities include, on one side, the consumer and the consumer's bank and, on the other, the merchant and the merchant's bank; between them are the credit card networks (e.g., VISA) and other third parties such as "independent sales organizations" involved in processing a transaction.

12. In 2012 and 2013, EPS served as the ISO for the entities involved in the MNF scam.

13. EPS engaged in the underwriting and approval of MNF's fictitious companies, and helped set up merchant accounts with its acquirer for these fictitious companies. Using the services of two payment processors, EPS enabled more than $4.6 million in MNF transactions to be processed through these and other fraudulent merchant accounts.

14. EPS used "sales agents" to market its processing services to merchants. Three of these sales agents, Jay Wigdore, Michael Abdelmesseh, and Nikolas Mihilli, directly participated in the MNF credit card laundering scheme.[1]

15. Wigdore submitted the merchant applications for the MNF fictitious companies to EPS, and EPS opened merchant accounts for them. MNF's transactions were then processed through the fictitious company accounts.

16. The MNF scam operated through a web of interrelated companies, including "Rose Marketing." When consumer complaints about MNF's scam mounted, threatening exposure of the scam, the principals and employees behind MNF changed the scheme's name and created new companies to continue operating the scam, under different and constantly changing names.

**The Money Now Funding Litigation**

17. The FTC filed an action against MNF and its related and successor companies on August 5, 2013, alleging that the deceptive and fraudulent business opportunity scam violated the FTC Act, the Business Opportunity Rule, and the Telemarketing Sales Rule. *FTC v. Money Now Funding, LLC, et al.*, CV 13-01583-PHX-ROS (D. Ariz. 2013). The complaint, which was amended on December 16, 2013, alleged, among other things, that MNF created fictitious companies supposedly owned by various MNF employees and applied for merchant accounts under these fictitious companies, and that MNF then used such merchant accounts to launder its credit card transactions.

18. In 2015, the FTC settled with many of the MNF defendants, obtaining court orders banning eighteen individual defendants from selling business or work-at-home opportunities. Also in 2015, the court granted the FTC's motion for summary judgment against certain MNF defendants, and entered default judgments

---

[1] The FTC brought an action in 2017 in federal court against two groups of defendants: (1) EPS, its owners, and an employee; and (2) Wigdore, his companies, and related companies and individuals. *FTC v. Electronic Payment Solutions of America, Inc., et al.*, No. CV-17-02535-PHX-SMM (D. Ariz., July 28, 2017). The following defendants settled claims with the FTC: Michael Peterson; Michael Abdelmesseh; Nikolas Mihilli and his company, Dynasty Merchants, LLC; and Jay Wigdore and his companies, Electronic Payment Solutions of America, Inc., and Electronic Payment Services, Inc. The Court granted summary judgment for the FTC against EPS, Dorsey and McCann as to liability under the FTC Act and the Telemarketing Sales Rule, but denied summary judgment as to the availability of injunctive relief. *See id.*, ECF No. 366 (Aug. 11, 2021). The FTC will dismiss that federal court complaint after the settlement of this administrative complaint is approved.

against the remaining MNF defendants, resulting in the entry of permanent injunctions and monetary judgments.

19. In granting the FTC's motion for summary judgment against MNF, the court found that MNF was a multi-million-dollar scheme to defraud consumers.

20. In 2016, the Arizona Attorney General's office brought criminal charges against four individuals involved in the MNF scam. As of January 25, 2017, all four had entered guilty pleas, with the lead defendant agreeing to a five-year prison term.

**Background on Credit Card Laundering**

21. In order to accept credit card payments from consumers, a merchant must establish a "merchant account" with a merchant acquiring bank (as noted above, also referred to as an "acquirer"). A merchant account is a type of account that allows businesses to process consumer purchases by a credit or debit card.

22. The acquirer is the entity that has access to the credit card associations (such as Mastercard and VISA), and through which merchant accounts are established. Without a merchant account obtained through an acquirer, merchants are unable to process consumer credit or debit card sales transactions.

23. Acquirers commonly enter into contracts with ISOs, who solicit and sign up merchants for merchant accounts with the acquirer. In some cases, ISOs engage in the screening and underwriting of prospective merchants, operate the acquirer's merchant processing program (directly or through the services of third-party processors), and monitor the merchants' transactions.

24. The credit card associations ("card networks"), such as VISA and Mastercard, require all participants in their networks, including the acquirers and their registered ISOs, to comply with detailed rules governing the use of the card networks. These rules include screening and underwriting merchants to ensure that they are legitimate bona fide businesses, and to screen out merchants engaged in potentially fraudulent or illegal practices. The rules also prohibit credit card laundering.

25. Merchants that pose a greater risk of fraud or financial loss to the ISO, acquirer, and card networks may be denied merchant accounts. For example, the ISO or acquirer may be concerned that the merchant is engaged in deceptive marketing, illegal activity or will generate excessive rates of transactions returned by consumers ("chargebacks").

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, fraudulent merchants can manipulate the system and avoid chargeback monitoring by spreading their transactions across multiple merchant accounts and ensuring that no single account has more than 100 chargebacks per month. They can also avoid

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, fraudulent merchants sometimes spread their transactions across multiple merchant accounts in order to circumvent the underwriting requirements or monitoring programs of the ISO's acquirer. For example, if the acquirer's underwriting rules are more lenient for merchants with lower projected sales volume, fraudulent merchants can artificially lower the merchant's projected sales volume by applying for numerous low-volume merchant accounts in the names of fictitious companies, thereby obtaining the acquirer's underwriting approval that the merchant otherwise would not be able to obtain.

34. By spreading out merchant transactions across numerous and constantly changing fraudulent merchant accounts over short time periods, fraudulent merchants and unscrupulous ISOs can cause an enormous amount of economic harm to consumers, before their transactions are detected or terminated by the ISO's acquirer or the card networks.

**Respondents' Acts and Practices Related to MNF Credit Card Laundering**

35. The MNF scam, in which consumer-victims were persuaded to make purchases over the telephone, relied on MNF having the ability to accept victim funds via credit and debit cards without raising fraud alerts. To conceal its identity and to prevent the acquirer and card networks from scrutinizing and terminating its merchant account, MNF engaged in a scheme with Wigdore and his associates to apply for at least 43 (forty-three) fraudulent merchant accounts, each under a different fictitious name, through which MNF could launder charges to consumers' credit or debit card accounts.

36. As part of this scheme, MNF created numerous fictitious companies, each using the name of a MNF principal or employee as the straw owner or purported principal of the company. These phony companies did not engage in any actual business. Thus, for example, one fictitious company was called "D&D Marketing," the supposed owner of which was actually an MNF employee with the initials "D.D." When consumer-victims signed up for the MNF business opportunity and made a payment, their credit card statements would show a charge made by a company they had never heard of, such as "D&D Marketing," rather than Money Now Funding.

37. In 2012, Wigdore, as a sales agent, submitted phony merchant applications on behalf of 23 MNF-related fictitious companies to EPS for EPS's underwriting approval.

38. When applying for a merchant account, merchants often submit with the application a copy of a voided check drawn on their business bank account, with the understanding that credit card sales revenues will be transferred into this account.

39. For each of the 23 fraudulent merchant applications, Wigdore attached a falsified voided preprinted check that purported to reflect the existence of a business bank account in the name of that fictitious company. Each check had been doctored to reflect an account holder, i.e., the fictitious company, that was not the true account holder for that account number. The account number printed on the bottom of each check corresponded with one of 23 different bank accounts at J.P. Morgan Chase Bank ("Chase"), each in the name of Dynasty Merchants, LLC, a company controlled by Wigdore's associate, Mihilli.

40. After receiving the fraudulent applications from Wigdore, EPS approved all 23 applications, set up merchant accounts for each fictitious company, and immediately began processing for these accounts through EPS's acquirer, Merrick Bank ("Merrick").

41. When MNF transactions were processed through the 23 fraudulent merchant accounts in the names of the fictitious companies, the sales revenues from these transactions were automatically transferred into the 23 Dynasty Chase Accounts, and subsequently transferred into a "Master Account" at the same bank, also held in the name of Dynasty.

42. From the Dynasty "Master Account," funds were divided up and eventually paid to a company owned by Wigdore, companies affiliated with the MNF scam, and individually to Abdelmesseh and Mihilli.

43. The scheme allowed MNF to obtain merchant accounts based on false information in the merchant applications. Specifically, each merchant application contained the following false information: (1) the name of the fictitious company was listed as the applicant, when the true applicant was the principal(s) of the MNF scam; (2) the name of the straw owner was listed as the owner of the business, when the true owner was the owner(s) of the MNF scam; and (3) the fictitious company was listed as the account holder of the merchant bank account, when the true account holder was Dynasty Merchants, LLC.

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 approximately 2004.[2] This relationship continued while Wigdore served a 57-month sentence on a federal fraud conviction from 2006 to 2009; during this period Wigdore's wife, Sandy Wigdore, continued acting as a sales agent for EPS.

48. EPS's principal, Respondent Thomas McCann, was aware of Wigdore's criminal history, but continued using Wigdore as EPS's sales agent.

49. EPS has held itself out as a processor for "High Risk" businesses that have difficulty finding banks willing to accept their business. EPS's website has stated that it had a "98% Approval Rate" for merchants who applied for its credit card processing services, as compared to its competitors who had a "60% Approval Rate."

---

[2] *Electronic Payment Transfer, LLC v. Federal Trade Commission and Citywide Banks*, No. 16-cv-1653 (D. Colo. filed June 28, 2016) was an action brought by EPS to enjoin a bank from complying with a civil investigative demand that the FTC had lawfully issued to the bank during its investigation of this matter. The case was dismissed in August 2016 upon agreement of the parties.

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 applications because the alleged principals of these merchants all shared the same email address as the principal of the merchant KMA Merchant Services, a Wigdore-related account owned by Wigdore's associate Michael Abdelmesseh, that Merrick had previously terminated. Merrick noted that the three declined merchants "have principal email addresses with the alias being at kmamarketingsvcs.com – KMA had chargeback issues with us in the past."

54. One week later, on May 31, 2012, Merrick declined yet another application, again informing Peterson that the merchant "also appears to be linked to KMA Marketing which has had chargeback issues with us."

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 merchants, the credit reports indicated that the principals or owners of the businesses had low credit scores, poor credit ratings, and owed substantial outstanding debts, raising obvious questions about the financial health of the merchants and the nature of their businesses. EPS nonetheless approved these merchants, without seeking to obtain additional information about the businesses or their financial viability.

d) Although Merrick's underwriting policy required EPS to obtain and evaluate samples of all relevant merchant marketing materials and telemarketing scripts, the 23 merchant applications did not include copies of the merchants' marketing materials.

e) Merrick's policy further required EPS to obtain screen prints of the relevant web pages of the merchant's website for "high risk" merchants such as telemarketers; however, for at least six merchant applications, the "Initial Risk Evaluation" conducted by EPS's employee specifically noted that the merchant did not have a valid merchant website.

f) For at least five merchant applications, the address listed on the credit report did not match the address listed for the merchant on the merchant application.

g) For at least five of the merchant applications, an attached Application Addendum form stated that "Jay Wigdore" was a co-owner or co-officer of the alleged merchant, in addition to another co-owner or co-officer whose name was listed on the application form.

h) For five merchants, the merchant's business bank account was listed on the application as "Comerica Bank," even though the checks attached to the applications indicated that the merchant's bank was Chase Bank, not Comerica Bank. Despite this obvious inconsistency, EPS nonetheless approved these applications.

58. Had EPS sought to verify the legitimacy of the 23 merchant bank accounts, it would have discovered that the true account holder for each of the 23

Chase bank accounts was not the company whose name was printed on the check and listed on the merchant application, but a different company: Dynasty Merchants, LLC.

59. Many of the merchant applications for the MNF-related merchants submitted by Wigdore contained clear indications that the merchants were engaged in telemarketing. For example, a section on the application form entitled "Merchant Product/Service Profile" asked "How is the Product or Service Ordered or Purchased (mail order, catalog, over the phone, in person, etc.)." The merchant applications contained the handwritten response "over the phone," indicating telemarketing.

60. Because telemarketers pose a higher risk of fraud, VISA rules require telemarketers to be classified and coded as "High Brand Risk Merchants." VISA rules further require that the correct Merchant Classification Code (or MCC) be assigned to all merchants. The MCC numbers 5966 and 5967 are used to indicate inbound and outbound telemarketers, which are High Brand Risk Merchants.

61. VISA imposes heightened monitoring requirements for all merchants that are coded as High Brand Risk Merchants, including merchants engaged in telemarketing. These monitoring requirements are designed to detect and prevent merchants from processing fraudulent or illegal credit card transactions through VISA's network.

62. Even though the merchant applications for many of the MNF-related merchants indicated that these entities were engaged in telemarketing, EPS concealed this fact by failing to assign to these entities the correct MCC number required for telemarketers. Instead, EPS entered MCC number 7311, which simply refers to "advertising services."

63. By not coding the MNF-related merchants as telemarketers and concealing this fact, EPS was able to avoid placing these merchants under the heightened monitoring program required by VISA for High Brand Risk Merchants.

64. Also, Merrick's underwriting policy and rules prohibited EPS from processing for telemarketers (and other categories of merchants deemed by EPS to be "high risk"), prior to obtaining Merrick's approval. Even though the applications indicated that many of the MNF-related merchants were engaged in telemarketing, EPS began processing for these entities prior to obtaining Merrick's approval, in direct violation of Merrick's rules.

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 range, so if you need to build a couple more accounts to reach your volume, please do so…"

80. The referenced merchant accounts ("the accounts that are on hold") included at least six of the MNF-related merchant accounts that EPS had opened and used to process MNF transactions.

81. With respect to one of these merchant accounts, Peterson placed an explicit note: "On Hold – Pay out Tuesday – Do not put any more volume for the month through this one!"

82. Because Merrick's underwriting rules or monitoring practices were in part based on a merchant's projected or actual sales volume, a fraudulent merchant might obtain Merrick's approval or avoid Merrick's scrutiny if it appeared to process a lower volume of transactions.

83. By knowingly processing transactions for the same underlying merchant (that is, MNF) through multiple merchant accounts opened in the names of the fictitious companies, Peterson directly engaged in credit card laundering. He knowingly concealed the true identity of the merchant (MNF). Peterson also engaged in tactics to evade Merrick's underwriting rules or monitoring practices and the card networks' chargeback monitoring programs, by spreading out the MNF transactions across multiple merchant accounts in order to artificially lower the volume of sales and chargeback transactions processed through any single merchant account.

84. In a February 21, 2013 email from KMA to an employee working in EPS's Risk Department, KMA provided EPS a list of address changes for numerous client merchants. The list clearly revealed that almost all of the MNF-related merchants, and numerous additional merchants, had changed their addresses to the same address (three post office boxes located at the same address in Phoenix,

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 processed at least $98,300 in transactions for these four fictitious companies combined. They also included fictitious companies controlled by managers of the MNF scam. One MNF manager, Cordell Bess, created a new fictitious company (Premier Online Marketing Strategies) to replace his previous fictitious company (JJB Marketing). In 2012, EPS had processed for JJB Marketing, until Merrick instructed EPS to terminate the company. The EPS employee who reviewed the application for Bess's new company (Premier Online Marketing Strategies) specifically noted that EPS already had opened a "previous account" for the same underlying merchant. EPS nonetheless approved the applications. About $62,795 in transactions was processed for this new fictitious company.

90. A second MNF manager, Cynthia Miller, also known as "Cynthia Metcalf" and "Cynthia Wilson," controlled at least 12 of the MNF-related fictitious companies from 2013. EPS approved the applications, and $1,666,003 in transactions was processed through the 12 Cynthia Miller-related accounts combined.

91. Peterson was fully aware that the Cynthia Miller-related entities were in fact related to the same underlying merchant or individual. In a spreadsheet attached to an email dated January 30, 2014 from Abdelmesseh ("Mike Stewart") to Mike Peterson, Abdelmesseh listed the names of the 12 merchants and the name of the straw owner of each merchant; the spreadsheet also indicated that all 12 merchants in fact belonged to a "Group" associated with one individual: "Cynthia Wilson."

92. EPS continued approving and processing for new merchants submitted by KMA and Wigdore, and continued processing for merchants previously referred to EPS by KMA, through at least the end of December 2013.

93. EPS's company practice of knowingly processing for merchants whose true identities were concealed was not limited to the MNF-related fictitious merchants. The practice applied to other merchants as well.

94. For example, in a September 17, 2013 email sent from EPS employee Chonda Pearson to an employee working in Wigdore's sales office, Pearson wrote: "Unfortunately this merchant has an open bankruptcy. We will be happy to process this deal with a new signer." Pearson's statement that the merchant circumvent Merrick's rules by simply finding a "new signer," is contrary to Merrick's underwriting policy that considered "any merchant that is currently in business bankruptcy" to be an "Unacceptable Merchant" for approval.

95. Similarly, in a May 20, 2013 email exchange between EPS employee Pearson and another employee in Wigdore's office, regarding a merchant called "M2M Gold," Pearson wrote: "This is the same signer—we need a different signer on the application." Pearson again reiterated this point two hours later, in a follow-up email, stating: "I spoke to Mike Peterson … We cannot do anything with it until we have a different signer."

96. Peterson and Abdelmesseh kept close track of the various merchants whose true identities were concealed behind different company names. For example, a spreadsheet attached to the January 30, 2014 email from "Mike Stewart" to Peterson listed numerous companies that belonged to particular "Groups." Each Group was associated with a single individual. For example, six merchants were in the "Group" associated with "Ryan Helms"; five "merchants" were in the "Group" associated with "Andrew Chavez"; six "merchants" were in the "Group" associated with "Ovi"; and 17 merchants were in the "Group" associated with "Lance Himes." Lance Himes was a former associate of MNF who had participated in the MNF scam.

97. EPS's employees were aware of complaints regarding various other deceptive marketing practices, not related to the MNF scam, engaged in by Wigdore and his associates. As early as December 19, 2011, one EPS employee emailed another EPS employee regarding a complaint received, stating: "New account we lost because Jay Wigdore lied."

98. In a February 22, 2012 email exchange between EPS employees regarding the "Wigdore accounts," one EPS employee discussed two merchants: "Both of merchants have similar story, doing 'lead generating' for Jay Wigdore . . . Dorothy Ventures isn't a business. Both ladies are retired, damn near 90. I talked to Jordan in Q&A and Travis about these accounts . . . both agreed the accounts were are most likely opened fraudulently by the agent(s)."

99. In another email exchange between EPS employees, dated March 28, 2012, one employee described a consumer complaint received regarding false promises made by the Wigdore sales agent: "They are promising trips/cruises/getaways etc to merchants for signing up with EPS." In reply, the other employee stated: "Yeah it's well-known at this point."

100. In another email exchange between EPS employees regarding "Jay Wigdore Accounts," dated September 11, 2012, one employee wrote: "We've seen an increase of non-installed merchants who are being signed up under false pretenses (agent 2088)."

101. EPS required Peterson, its Risk Manager, to closely track EPS's client merchants' sales and chargeback transaction activity on a regular basis. As noted above, various emails indicate that Peterson knew a great deal about the fraudulent nature of the businesses in which KMA and MNF were engaged, and their credit card laundering activities. Peterson received emails from Merrick in 2012, discussed above, in which Merrick expressed concern about KMA's high chargeback rate "and the reason codes for them (services not provided)" and in which Merrick expressed the opinion that KMA was engaged in the unlawful practice of "load balancing." In another email, Peterson said EPS should not fight a chargeback dispute involving a charge in the name of KMA Merchant Services for a "Rose Marketing" transaction, because "the argument against factoring is too great." In another email, Peterson directly instructed Abdelmesseh, acting in his capacity as sales agent, to "spread out" KMA's client merchant's transactions across multiple merchant accounts opened in the names of several MNF-related fictitious merchants. Peterson was fully aware that many of the merchant accounts were related to the same underlying merchant or individual.

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. McCann and Dorsey personally met and communicated directly with the sales agents Wigdore and Abdelmesseh. They each approved numerous merchant applications for the MNF-related merchants referred by Wigdore—applications that contained glaring signs that the companies were not legitimate businesses and were related to each other or to the same underlying merchant and, therefore, were likely being used to launder transactions for another merchant.

106. Dorsey personally approved numerous MNF-related merchant applications. On one, Wigdore appeared as a co-owner or co-officer of the merchant, and the merchant did not have a business website, and owed a "past due amount" of $20,225. Dorsey approved another application even though the merchant did not have a business website and owed a "past due amount" of $139,463. Dorsey approved yet another merchant who did not have a business website, owed a "past due amount" of $10,914, and whose credit report provided an address that did not match the address on the application.

107. On July 24, 2012, Dorsey approved a merchant despite the merchant's incorporation papers showing that it had different owners and a different business address than those listed on the application. Moreover, an EPS employee had specifically noted that the merchant shared the same address as another EPS client merchant (JJB Marketing). EPS had processed for JJB Marketing just one month before, until Merrick instructed it to terminate the merchant. Despite knowing that the new merchant was related to the previous client merchant, Dorsey approved the application.

108. Similarly, McCann approved numerous MNF-related merchant applications, including eight applications submitted by Wigdore within a span of just two days (May 17, 2012 – May 18, 2012), two of which explicitly stated that

Wigdore was a co-owner or co-officer of the merchant, and five of which stated that the merchant had the exact same "KMA" email address. McCann approved two applications for merchants that shared a business address, a fact highlighted by the EPS employee who conducted the "initial risk evaluation" of the merchants.

109. McCann and Dorsey closely monitored the referral of new merchants to EPS by EPS's sales agents, as evidenced in daily emails (titled "Daily Hot Sheets") sent by EPS employees to McCann and Dorsey throughout 2013. These Daily Hot Sheets provided McCann and Dorsey a daily log of all new merchants approved by EPS for processing, and identified the sales agent who referred the merchant to EPS. The Daily Hot Sheets indicated that "Agent 2088" was among EPS's top sales agents, referring the highest number of merchant applications to EPS throughout 2013.

110. In addition to receiving fees or commissions for opening the MNF-related fictitious merchants' accounts and processing transactions through them, EPS transferred a substantial amount of MNF merchant funds (derived from MNF credit card sales generated by 16 of the fraudulent merchant accounts) into EPS's own bank accounts, which were jointly owned and controlled by Dorsey and McCann.

111. More than $4.6 million in sales transactions were processed through the MNF-related merchant accounts. These amounts do not include funds returned to consumers in the form of refunds or chargebacks.

112. Many of the consumers whose credit cards were charged never obtained a refund or reversed charge for the unauthorized charges. Even those consumers who ultimately received a refund or reversed charge for the unauthorized charges were forced to expend valuable time and energy in requesting and seeking the refunds or chargebacks. In addition, these consumers' banks and the card networks also have incurred substantial economic harm as a result of expending time and energy processing requests for refunds or chargebacks.

113. Consumers who directly suffered economic harm as a result of the Respondents' actions could not reasonably have avoided such harm because (a) they were deceived by the deceptive telemarketing practices of the MNF scam, (b) they never authorized the MNF scam or Respondents to charge their credit card accounts in the names of the MNF-related fictitious merchants, and (c) they had neither knowledge of nor control over the Respondents' actions in creating the MNF-related fictitious merchants' accounts through which Respondents processed MNF charges to the consumers' credit card accounts.

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 the credit card industry marketplace from the Respondents' conduct because no legitimate business purpose exists for credit card laundering.

**The Telemarketing Sales Rule**

115. Congress directed the FTC to prescribe rules prohibiting abusive and deceptive telemarketing acts or practices pursuant to the Telemarketing Act, 15 U.S.C. §§ 6101-6108. The FTC adopted the original Telemarketing Sales Rule in 1995, extensively amended it in 2003, and amended certain provisions thereafter. 16 C.F.R. Part 310.

116. Pursuant to Section 3(c) of the Telemarketing Act, 15 U.S.C. § 6102(c) and Section 18(d)(3) of the FTC Act, 15 U.S.C. § 57a(d)(3), a violation of the TSR constitutes an unfair or deceptive act or practice in or affecting commerce, in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

117. Under the TSR, a "merchant" means a person who is authorized under a written contract with an acquirer to honor or accept credit cards, or to transmit or process for payment credit card payments, for the purchase of goods or services or a charitable contribution. 16 C.F.R. § 310.2(u).

118. The MNF-related merchants were "merchants" who entered into "merchant agreements," as those terms are defined by the TSR, 16 C.F.R. § 310.2(u)–(v).

119. The MNF-related merchants were "seller[s]" or "telemarketer[s]" engaged in "telemarketing," as those terms are defined in the TSR, 16 C.F.R. §§ 310.2(dd), (ff), and (gg).

120. Except as expressly permitted by the applicable credit card system, it is a deceptive telemarketing act or practice for:

a) a merchant to present to or deposit into, or cause another to 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; or

b) any person to employ, solicit, or otherwise cause a merchant, or an employee, representative or agent of the merchant, to

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 numerous fictitious companies for the same underlying merchant, thereby concealing the true identity of the underlying merchant; and/or

c) Permitting the continued processing of transactions for the same underlying merchant through multiple merchant accounts opened in the names of numerous fictitious companies after being informed that the accounts should be shut down.

123. Respondents' actions caused or were likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves. This practice is an unfair act or practice.

**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 10th day of May, 2022, has issued this Complaint against Respondents.

By the Commission.

April J. Tabor
Secretary

SEAL:

**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.

**Decision and Order**

**Docket No. C-4764**

## DECISION

The Federal Trade Commission ("Commission") initiated an investigation of certain acts and practices of the Respondents named in the caption. The Commission's Bureau of Consumer Protection ("BCP") prepared and furnished to Respondents a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge the Respondents with violations of the Federal Trade Commission Act.

Respondents and BCP thereafter executed an Agreement Containing Consent Order ("Consent Agreement"). The Consent Agreement includes: 1) statements by Respondents that they neither admit nor deny any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, they admit the facts necessary to establish jurisdiction; and 2) waivers and other provisions as required by the Commission's Rules.

The Commission considered the matter and determined that it had reason to believe that Respondents have violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of 30 days for the receipt and consideration of public comments. The Commission duly considered any comments received from interested persons pursuant to Section 2.34 of its Rules, 16 C.F.R. § 2.34. Now, in further conformity with the procedure prescribed in Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

**Findings**

1. The Respondents are:

    a) Respondent Electronic Payment Systems, LLC, also doing business as EPS, a Colorado limited liability company with its principal office or place of business at 6472 S. Quebec St., Englewood, CO 80111.

    b) Respondent Electronic Payment Transfer, LLC, also doing business as EPS, a Colorado limited liability company with its principal office or place of business at 6472 S. Quebec St., Englewood, CO 80111.

    c) Respondent John Dorsey, an officer of the Proposed Corporate Respondents, Electronic Payment Systems, LLC and Electronic Payment Transfer, LLC. His principal office or place of business is the same as that of Electronic Payment Systems, LLC and Electronic Payment Transfer, LLC.

    d) Respondent Thomas McCann, an officer of the Proposed Corporate Respondents, Electronic Payment Systems, LLC and Electronic Payment Transfer, LLC. His principal office or place of business is the same as that of Electronic Payment Systems, LLC and Electronic Payment Transfer, LLC.

2. The Commission has jurisdiction over the subject matter of this proceeding and of Respondents, and the proceeding is in the public interest.

## ORDER

### Definitions

For the purposes of this Order, the following definitions apply:

1. "Acquirer" means a business organization, Financial Institution, or an agent of a business organization or Financial Institution that has authority from an organization that operates or licenses a credit card system (e.g. VISA, Inc., MasterCard, Inc., American Express Company, and Discover Financial Services, Inc.) to authorize Merchants to accept, transmit, or process payment by credit card through the credit card system for money, products or services, or anything else of value. The EPS Respondents are not considered to be Acquirers.

2. "Additional Review Merchant" means any Merchant that:

   a) Engages in Outbound Telemarketing; or

   b) Offers to sell, sells, promotes, or markets any of the following products or services by any means: debt collection, debt relief, consumer credit related services, rental housing listings, job listings or Money Making Opportunities.

3. "Chargeback" means a procedure whereby an issuing bank or other Financial Institution charges all or part of an amount of a Person's credit or debit card transaction back to the Acquirer or other Financial Institution.

4. "Chargeback Rate" means the proportion (expressed as a percentage) of Chargebacks out of the total number of attempted credit or debit card sales transactions.

5. "Credit Card Laundering" means:

   a) Presenting or depositing into, or causing or allowing another to present or deposit into, the credit card system for payment, a Credit Card Sales Draft generated by a transaction that is not the result of a credit card transaction between the cardholder and the Merchant;

b) Employing, soliciting, or otherwise causing or allowing a Merchant, or an employee, representative, or agent of a Merchant, to present to or deposit into the credit card system for payment, a Credit Card Sales Draft generated by a transaction that is not the result of a credit card transaction between the cardholder and the Merchant; or

c) Obtaining access to the credit card system through the use of a business relationship or an affiliation with a Merchant, when such access is not authorized by the Merchant Account agreement or the applicable credit card system.

6. "Credit Card Sales Draft" means any record or evidence of a credit card transaction.

7. "EPS Merchant" means any Person:

a) Who obtains, directly or indirectly, from any EPS Respondent a Merchant Account; or

b) To whom any EPS Respondent provides, directly or indirectly, Payment Processing services.

8. "Financial Institution" means any institution engaged in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. § 1843(k)). An institution that is significantly engaged in financial activities is a Financial Institution.

9. "Fraud Monitoring" or "Risk Monitoring Program" means any program established to monitor or detect potentially fraudulent, illegal, or unauthorized Merchant transactions and activity by a credit card association (e.g., VISA, MasterCard, American Express, Discover), Acquirer, Financial Institution, or operator of a payment system. Such programs include any program established to monitor Chargebacks (including VISA's Merchant Chargeback Monitoring Program) or Chargeback Rates, reasons provided for Chargeback transactions (e.g., VISA's Merchant Chargeback Monitoring Program), fraudulent or unauthorized transactions (e.g., MasterCard's "GMAP Program," VISA's Risk Identification Service program), and Merchants classified or defined by VISA as high risk Merchants (however titled), including VISA's "High Brand Risk Merchant" program, as periodically revised or updated from time to time.

10. "Independent Sales Organization" or "ISO" means any Person that:

a) Enters into an agreement or contract with a Payment Processor, Acquirer or Financial Institution to sell or market Payment Processing services to a Merchant;

b) Matches or refers Merchants to a Payment Processor or Acquirer for Payment Processing services, or that matches or refers a Payment Processor or Acquirer to Merchants for Payment Processing services; or

c) Is registered as an ISO or merchant service provider ("MSP") with VISA, MasterCard, or any credit card association.

11. "Merchant" means any Person engaged in the sale or marketing of any products or services or a charitable contribution, including any Person who applies for Payment Processing services.

12. "Merchant Account" means any account with an Acquirer or other Financial Institution, service provider, Payment Processor, ISO, or other entity that enables an individual, a business, or other organization to accept credit card, debit card, or check payments of any kind.

13. "Money Making Opportunity" means a business model in which a Merchant offers to sell, sells, promotes, or markets any product or service represented to enable consumers or to assist consumers in:

a) Earning income through a work-from-home business opportunity;

b) Obtaining training or education on how to establish a business or earn money or other consideration through a business;

c) Obtaining employment for an upfront fee; or

d) Obtaining government grants or other government income, benefits, or scholarships.

The term "Money Making Opportunity" does not include services provided by a school or program of instruction that has been evaluated and found to meet established criteria by an accrediting agency or association recognized for such purposes by the U.S. Department of Education.

14. "Outbound Telemarketing" means any plan, program, or campaign that is conducted to induce the purchase of products or services by use of one or more telephones, and which involves a telephone call initiated by a Person other than the consumer.

15. "Payment Processing" means transmitting sales transaction data on behalf of a Merchant or providing a Person, directly or indirectly, with the means used to charge or debit accounts through the use of any payment method or mechanism, including credit cards, debit cards, prepaid cards, and stored value cards. Whether accomplished through the use of software or otherwise, Payment Processing includes, among other things:

a) Reviewing and approving Merchant applications for payment processing services;

b) Transmitting sales transaction data or providing the means to transmit sales transaction data from Merchants to Acquirers, Payment Processors, ISOs, or other Financial Institutions;

c) Clearing, settling, or distributing proceeds of sales transactions from Acquirers or Financial Institutions to Merchants; or

d) Processing Chargebacks.

16. "Payment Processor" means any Person providing Payment Processing services in connection with another Person's sale of products or services, or in connection with any charitable donation.

17. "Person" means any natural person, or any entity, corporation, partnership, or association of Persons.

18. "Respondents" means all of the Corporate Respondents and the Individual Respondents, individually, collectively, or in any combination.

a) "Corporate Respondents" means Electronic Payment Systems, LLC and Electronic Payment Transfer, LLC, both also doing business as EPS, and their successors and assigns.

b) "Individual Respondents" means John Dorsey and Thomas McCann.

19. "Sales Agent" means a Person that:

a) Enters into an agreement or contract with an ISO to sell or market Payment Processing services to a Merchant; or

b) Matches or refers Merchants to an ISO for Payment Processing services, or that matches or refers an ISO to Merchants for Payment Processing Services.

As such, a Sales Agent may be involved in recommending a particular ISO to a Merchant, forwarding to the ISO a Merchant's application, or negotiating rates and fees charged by an ISO.

## Provisions

### I.
### Prohibitions Against Deceptive or Unfair Payment Processing Acts or Practices

**It is ordered that** Respondents, and Respondents' officers, agents, and employees, and those other persons in active concert or participation with any of them, who receive actual notice of this Order by personal service or otherwise, whether acting directly or indirectly, in connection with offering Payment Processing services, must not:

A. Engage in Credit Card Laundering;

B. Engage in tactics to evade any Fraud Monitoring or Risk Monitoring Program, including:

1) Making, or assisting others in making any false or misleading statement, or providing any false document, in order to obtain a Merchant Account or Payment Processing services;

2) Opening multiple Merchant Accounts in the names of other companies for the same underlying Merchant, in order to conceal the Merchant's true identity;

3) Processing a Merchant's credit card transactions through multiple Merchant Accounts opened in the names of other companies, in order to artificially alter the true volume of transactions processed through any single Merchant Account;

4) Misrepresenting whether a Merchant is engaged in Outbound Telemarketing; and

5) Using or providing a bank account set up for the purpose of receiving only the returned transactions of any payment instrument (including checks and credit card transactions), in order to conceal Chargeback levels of Merchant transactions deposited into a different bank account;

C. Provide Payment Processing services to any Merchant that is engaged in any act or practice that is, or is likely to be, deceptive or unfair, including:

1) The unauthorized charging of consumer credit card accounts or the unauthorized debiting of consumer bank accounts;

2) The misrepresentation, directly or by implication, of the total costs to purchase, receive, or use any product or service; any material aspect of the performance, efficacy, nature, or central characteristics of the product or service; and any material aspect of the nature of the Merchant's refund, cancellation, exchange, or repurchase policies;

3) The failure to disclose, clearly and conspicuously, the total cost to purchase, receive or use any product or service;

4) Any tactics to conceal the true identity of the Merchant, including the use of shell companies or fictitious company names to conduct business, in order to gain access to a payment network, apply for Payment Processing services, or apply for Merchant Accounts;

5) Any tactics to evade any Fraud Monitoring or Risk Monitoring Program, including: distributing sales transaction volume among multiple Merchant Accounts or splitting a single sales transaction into multiple smaller transactions, in order to conceal a Merchant's identity or to artificially alter the true volume of transactions processed through any single Merchant Account;

6) Making any false or misleading statement, or providing any false document, in order to obtain a Merchant Account or Payment Processing services; and

7) Misrepresenting the type of business engaged in by the Merchant, or the means of advertising, marketing, and sales used by the Merchant (i.e., whether the Merchant is engaged in Outbound Telemarketing); and

D. Provide Payment Processing services or acting as an ISO or Sales Agent for any Merchant that is listed on the MasterCard Member Alert to Control High-Risk Merchants (MATCH) list for any of the following reasons:

1) Excessive chargebacks,

2) Fraud,

3) Identification as a Questionable Merchant per the MasterCard Questionable Merchant Audit Program,

4) Merchant collusion,

5) Illegal transactions,

6) Credit Card Laundering, or

7) Identity theft.

**II.**
**Screening of Additional Review Merchants**

**It is further ordered that** Respondent, and Respondents' officers, agents, and employees, and those other persons in active concert or participation with any of them, who receive actual notice of this Order by personal service or otherwise, whether acting directly or indirectly, in connection with offering Payment Processing services, must engage in reasonable screening of Additional Review Merchants to confirm each Additional Review Merchant's identity, and to determine whether each Additional Review Merchant's business practices are, or are likely to be, deceptive or unfair.

Such reasonable screening must include:

A. Establishing and maintaining policies and procedures designed to identify Merchants that qualify as Additional Review Merchants;

B. Obtaining from each Additional Review Merchant:

1) A description of the nature of the Additional Review Merchant's business, including the nature of the products and services for which the Additional Review Merchant seeks Payment Processing services, and a description of the means of advertising, marketing, and sales used (i.e., Outbound Telemarketing, Internet sales);

2) The name(s) of the principal(s) and controlling Person(s) of the entity, and of Person(s) with a twenty-five percent (25%) or greater ownership interest in the entity;

3) A list of all business names, trade names, aliases or fictitious names, DBAs, websites, and identification numbers (such as taxpayer ID numbers) under or through which the Additional Review Merchant is marketing or intends to market the products and services for which the Additional Review Merchant seeks Payment Processing services;

4) Each physical address at which the Additional Review Merchant conducts business or will conduct the business(es) identified pursuant to subsection (1) of this Section II.B;

5) A list of all postal addresses, email addresses, telephone numbers, and Internet addresses the Additional Review Merchant uses or will use to conduct the business(es) identified pursuant to subsection (1) of this Section II.B;

6) For each product or service for which the Additional Review Merchant seeks Payment Processing services, the bank account number and name of the account holder(s) for each depository bank account currently held by the Additional Review Merchant and into which the Additional Review Merchant's sales revenues are to be deposited, and the name of the bank(s) at which each such depository bank account is maintained;

7) The percentage of the Additional Review Merchant's sales transactions, for which the Additional Review Merchant seeks Payment Processing services, that qualify as "Card Not Present Transactions," and a detailed breakdown of the Additional Review Merchant's different types of "Card Not Present

Transactions" (i.e., Internet or ecommerce sales, Outbound Telemarketing);

8) Representative samples of all types of current marketing materials, including, but not limited to screen prints of relevant web pages and public social media pages, for the products or services for which the Additional Review Merchant seeks Payment Processing services;

9) Copies of all fulfillment agreements, if the Additional Review Merchant utilizes third party fulfillment providers;

10) Information regarding whether the Additional Review Merchant, including the principal(s) and controlling Person(s) of the Additional Review Merchant entity, any Person(s) who has a twenty-five percent (25%) or greater ownership interest in the entity, and any corporate name, trade name, fictitious name or aliases under which such Person(s) conduct or has conducted business, has ever been:

    a) Placed in any Fraud Monitoring or Risk Monitoring Program;

    b) Listed on the MasterCard Member Alert to Control High-Risk Merchants ("MATCH") list;

    c) Placed in a payment card association's chargeback monitoring program; or

    d) The subject of legal action taken by the Commission or any other state or federal law enforcement agency;

11) Copies of monthly or periodic Payment Processing statements issued by each bank, Acquirer, Payment Processor, ISO, or Sales Agent used by the Additional Review Merchant during the preceding three (3) months, to the extent the Additional Review Merchant used Payment Processing services in the preceding three (3) months; and

12) The Additional Review Merchant's past Chargeback Rates for the preceding three (3) months, to the extent the Additional

Review Merchant used Payment Processing services in the preceding three (3) months;

C. Taking reasonable steps to assess the accuracy of the information provided pursuant to Section II.B of this Order, and to confirm the identity of the Additional Review Merchant, including:

1) Subject to any limitations put in place by the Financial Institution that carries the account, confirming the Additional Review Merchant's depository bank account(s), including requesting and reviewing bank reference or bank verification letters;

2) Cross-referencing the following information relating to the Additional Review Merchant with similar information associated with other Merchants in Respondent Electronic Payment Systems' current Merchant portfolio, in order to determine whether the Additional Review Merchant has concealed or attempted to conceal its true identity, or is related to or associated with any other Merchant in Electronic Payment Systems' current Merchant portfolio or any other Merchant previously approved by Electronic Payment Systems that was referred by the same Sales Agent:

a) The Additional Review Merchant's business names, trade names, aliases or fictitious names, DBAs, and identification numbers (such as taxpayer identification numbers);

b) The Additional Review Merchant's physical addresses, postal addresses, email addresses, Internet addresses, websites, telephone numbers, and bank accounts; and

c) The names of the principal(s) and controlling Person(s) of the Additional Review Merchant, and of Person(s) with a twenty-five percent (25%) or greater ownership interest in the Additional Review Merchant;

3) Reviewing copies of monthly or periodic Payment Processing statements issued by any bank, Acquirer, Payment Processor, ISO, or Sales Agent used by the Additional Review Merchant during the preceding three (3) months;

4) Reviewing representative samples of all current marketing materials, including, but not limited to screen prints of relevant web pages and public social media pages, and all fulfillment agreements provided by the Additional Review Merchant, for the products or services for which the Additional Review Merchant seeks Payment Processing services;

5) Reviewing credit reports of the Additional Review Merchant and Person(s) with a twenty-five percent (25%) or greater ownership interest in the entity; and

6) Reviewing background information regarding the Additional Review Merchant, its principal(s) and controlling Person(s) of the entity, and of Person(s) with a twenty-five percent (25%) or greater ownership interest in the entity.

D. The purpose of the reasonable screening process described in Section II.A through C is to:

1) Confirm that the Additional Review Merchant is engaged in offering the products and services, and using the means of advertising, marketing, and sales, that are described in its application for Payment Processing services;

2) Determine whether the Additional Review Merchant has attempted to conceal its true identity, and is likely engaged in Credit Card Laundering;

3) Determine whether the Additional Review Merchant's past transactions exhibit any unusual or suspicious transaction patterns, trends, values, and volume, including processing for time periods of less than three months or processing only during alternating months, for no apparent legitimate business reason or lawful purpose;

4) Determine whether the Additional Review Merchant has likely engaged in tactics to evade any Fraud Monitoring or Risk Monitoring Program, including opening and processing through multiple Merchant Accounts in order to artificially alter its true total volume of sales transactions or Chargebacks processed through any one single Merchant Account, or for no apparent legitimate business reason or lawful purpose;

5) Determine whether the Additional Review Merchant is engaged in any of the following unfair or deceptive acts or practices:

a) Failing to clearly and conspicuously disclose the total cost to purchase, receive, or use, any products or services;

b) Misrepresenting any material aspect of the performance, efficacy, nature, or central characteristics of products or services;

c) Failing to clearly and conspicuously disclose all material terms and conditions of an offer;

d) Misrepresenting, expressly or by implication, any material aspect of the Additional Review Merchant's refund, cancellation, exchange, or repurchase policies; and

e) Causing billing information to be submitted for payment without the customer's express authorization.

## III.
## Monitoring of Additional Review Merchants

**It is further ordered that** Respondent, and Respondent's officers, agents, and employees, and those other persons in active concert or participation with any of them, who receive actual notice of this Order by personal service or otherwise, whether acting directly or indirectly, in connection with offering Payment Processing services, must:

A. Monitor the sales activity of all current EPS Merchants to identify EPS Merchants that should be designated as Additional Review Merchants requiring additional screening pursuant to Section II of this Order, and for those EPS Merchants that become designated as Additional Review Merchants, complete the additional screening process described in Section II of this Order within 10 days of the date the EPS Merchant is determined to be an Additional Review Merchant;

B. Monitor each Additional Review Merchant's marketing practices and sales transactions to determine whether the Additional Review Merchant is engaged in practices that are deceptive or unfair in violation of Section 5 of the FTC Act. Such

monitoring must include reviewing Additional Review Merchants' websites; reviewing each Additional Review Merchant's Chargeback Rates and reasons provided for these rates, as well as examining any unusual or suspect transaction patterns, values, and volume; reviewing each Additional Review Merchant's consumer complaints related to requests for Chargebacks and complaints found on publicly available complaint mediums (i.e., online consumer complaint boards), or received from any third party, including Financial Institutions, credit card associations, Better Business Bureaus, and operators of payment systems;

C. Monitor each Additional Review Merchant's accounts to detect indicia that the Additional Review Merchant is engaged in Credit Card Laundering, tactics to conceal its true identity, or tactics to evade any Fraud Monitoring or Risk Monitoring Program. Such indicia include:

1) Unusual or suspicious transactions, patterns, trends, values, and volume;

2) Opening and closing multiple Merchant Accounts for the same underlying Merchant under different business names, for no apparent legitimate business or lawful purpose;

3) Payment Processing of transactions through Merchant Accounts for time periods of less than three months, or during only alternating months, for no apparent legitimate business or lawful purpose;

4) Distributing sales transaction volume across multiple Merchant Accounts of any payment system; and

5) Using an incorrect Merchant Category Code;

D. Calculate and update the Chargeback Rate at least on a monthly basis for each Additional Review Merchant. The Chargeback Rate must be calculated separately for each payment mechanism processed, including credit and debit card transactions. For any Additional Review Merchant with multiple Merchant Accounts, the calculation of the Chargeback Rate must be made for each of the Additional Review Merchant's individual accounts, and in the aggregate for each Additional Review Merchant;

E. Immediately conduct a reasonable investigation of the cause of Chargeback Rates for any Additional Review Merchant whose monthly Chargeback

Rate exceeds one percent (1%) and whose total number of Chargebacks exceeds fifty-five (55) per month in any two of the past six months, as follows:

1) Updating the information gathered in compliance with Section II of this Order, as applicable, and any other advertising of the Additional Review Merchant, and confirming the accuracy thereof;

2) Confirming that the Additional Review Merchant has obtained required consumer authorizations for the transactions;

3) Reviewing the consumer complaints and reasons provided for all Chargeback transactions;

4) If contact information is available, contacting consumers, Financial Institutions, and Better Business Bureaus to gather detailed information, including complaints and other relevant information, regarding the Additional Review Merchant;

5) Reviewing websites used by the Additional Review Merchant to market its products and services;

6) Searching publicly available sources for consumer complaints against the Additional Review Merchant alleging fraud (including online consumer complaint boards), and for legal actions against the Additional Review Merchant undertaken by the Commission or other state or federal law enforcement agencies;

7) Conducting "test" shopping to determine the Additional Review Merchant's sales practices, where possible; and

8) Stopping the processing of sales transactions and closing all processing accounts for any Additional Review Merchant investigated pursuant to this Subsection III.E within 30 days of commencing the investigation, unless the EPS Respondents draft a written report establishing facts that demonstrate that the Additional Review Merchant's business practices are not deceptive or unfair in violation of Section 5 of the FTC Act and are not in violation of the Telemarketing Sales Rule.

F. Immediately stop processing sales transactions and close all Merchant Accounts for any Additional Review Merchant that the EPS Respondents know or should know is engaged in Credit Card Laundering, tactics to conceal its true identity, or tactics to evade any Fraud Monitoring or Risk Monitoring Program, including balancing or distributing sales transaction volume or sales transaction activity among multiple Merchant Accounts or merchant billing descriptors; splitting a single sales transaction into multiple transactions, or using shell companies to apply for additional Merchant Accounts.

Nothing in this Section III should be read to insulate the EPS Respondents from liability for a violation of Section 5 of the FTC Act, the TSR, or any provision of this Order.

## IV.
## Monitoring of Sales Agents and Termination of Sales Agents Engaged in Certain Practices

**It is further ordered that** Respondents, and Respondents' officers, agents, and employees, and those other persons in active concert or participation with any of them, who receive actual notice of this Order by personal service or otherwise, whether acting directly or indirectly, in connection with offering Payment Processing services, in connection with offering or providing Payment Processing services, must:

A. Monitor each Sales Agent's past referral of Merchants and existing Merchant portfolio to determine whether any Merchant referred by the Sales Agent has engaged in tactics to conceal its true identity or is related to or associated with any other Merchant previously referred to any EPS Respondent by the same Sales Agent;

B. Immediately terminate the EPS Respondents' relationship with any Sales Agent as soon as practicable and in no more than 3 days, for any Sales Agent that any EPS Respondent knows or should know:

1) Has provided false information or false documents to apply for Payment Processing services or a Merchant Account for any Merchant, that the Sales Agent knew or should have known was false;

2) Has referred Merchants to any EPS Respondent that the Sales Agent knew or should have known were concealing their true

identities, or are engaged in or have been engaged in deceptive or unfair sales practices;

3) Has engaged in Credit Card Laundering or any tactics to evade any Fraud Monitoring or Risk Monitoring Program; or

4) Is or has been engaged in deceptive or unfair sales practices.

## V.
## Acknowledgments of the Order

**It is further ordered that** Respondents obtain acknowledgments of receipt of this Order:

A. Each Respondent, within 10 days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.

B. For 5 years after the issuance date of this Order, each Individual Respondent for any business that such Respondent, individually or collectively with any other Respondents, is the majority owner or controls directly or indirectly, unless such business cannot violate the Order, and each Corporate Respondent, must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities for conduct related to the subject matter of the Order and all agents and representatives who participate in conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Reports and Notices. Delivery must occur within 10 days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.

C. From each individual or entity to which a Respondent delivered a copy of this Order, that Respondent must obtain, within 30 days, a signed and dated acknowledgment of receipt of this Order.

## VI.
## Compliance Reports and Notices

**It is further ordered that** Respondents make timely submissions to the Commission:

A. One year after the issuance date of this Order, each Respondent must submit a compliance report, sworn under penalty of perjury, in which:

1) Each Respondent must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission, may use to communicate with Respondent; (b) identify all of that Respondent's businesses that could violate the Order by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business, including the products and services offered, the means of advertising, marketing, and sales, and the involvement of any other Respondent (which Individual Respondents must describe if they know or should know due to their own involvement); (d) describe in detail whether and how that Respondent is in compliance with each Provision of this Order, including a discussion of all of the changes the Respondent made to comply with the Order; and (e) provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.

2) Additionally, each Individual Respondent must: (a) identify all his telephone numbers and all his physical, postal, email and Internet addresses, including addresses used for any business; (b) identify all his business activities, including any business for which such Respondent performs services whether as an employee or otherwise and any entity in which such Respondent has any ownership interest; and (c) describe in detail such Respondent's involvement in each such business activity, including title, role, responsibilities, participation, authority, control, and any ownership.

B. For 10 years after the issuance date of this Order, each Respondent must submit a compliance notice, sworn under penalty of perjury, within 14 days of any change in the following:

1) Each Respondent must submit notice of any change in: (a) any designated point of contact; or (b) the structure of any Corporate Respondent or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.

2) Additionally, each Individual Respondent must submit notice of any change in: (a) name, including alias or fictitious name, or residence address; or (b) title or role in any business activity, including (i) any business for which such Respondent performs services whether as an employee or otherwise and (ii) any entity in which such Respondent has any ownership interest and over which Respondents have direct or indirect control. For each such business activity, also identify its name, physical address, and any Internet address.

C. Each Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against such Respondent within 14 days of its filing.

D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: "I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____" and supplying the date, signatory's full name, title (if applicable), and signature.

E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: *In re Electronic Payment Systems, LLC*, matter number 1523213.

## VII.
## Recordkeeping

**It is further ordered that** Respondents must create or receive, as applicable, certain records for 10 years after the issuance date of the Order, and retain each such record for 5 years. Specifically, Corporate Respondents in connection with offering or providing Payment Processing services, and each Individual Respondent for any business that such Respondent, individually or collectively with any other Respondents, is a majority owner or controls directly or indirectly, must create and retain the following records:

A. Accounting records showing the revenues from all products or services sold that are related to the subject matter of the Order;

B. Personnel records showing, for each person providing services in relation to any aspect of the Order, whether as an employee or otherwise, that person's: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;

C. Records of all EPS Merchant files and transactions, including Merchant Applications, underwriting documents, screening and monitoring records, investigation records and reports, bank verification records, processed transactions, and Chargeback transactions;

D. Records of all consumer complaints concerning the subject matter of the Order, including Chargeback requests, Chargeback dispute documentation, and refund requests with respect to EPS Merchants, whether received directly or indirectly, such as through a third party, and any response; and

E. All records necessary to demonstrate full compliance with each provision of this Order, including all submissions to the Commission.

## VIII.
## Compliance Monitoring

**It is further ordered that**, for the purpose of monitoring Respondents' compliance with this Order:

A. Within 14 days of receipt of a written request from a representative of the Commission, each Respondent must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury, and produce records for inspection and copying.

B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with each Respondent. Respondents must permit representatives of the Commission to interview anyone affiliated with any Respondent who has agreed to such an interview. The interviewee may have counsel present.

C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondents or any individual or entity affiliated with Respondents, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

D. Upon written request from a representative of the Commission, any consumer reporting agency must furnish consumer reports concerning Individual Respondents, pursuant to Section 604(2) of the Fair Credit Reporting Act, 15 U.S.C. § 1681b(a)(2).

## IX.
## Order Effective Dates

**It is further ordered that** that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate 20 years from the date of its issuance (which date may be stated at the end of this Order, near the Commission's seal), or 20 years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

A. Any Provision in this Order that terminates in less than 20 years;

B. This Order's application to any Respondent that is not named as a defendant in such complaint; and

C. This Order if such complaint is filed after the Order has terminated pursuant to this Provision.

*Provided, further*, that if such complaint is dismissed or a federal court rules that the Respondent did not violate any provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that

the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

April J. Tabor
Secretary

Seal:

Issued: May 10, 2022