DAVID SHONKA
Federal Trade Commission
Acting General Counsel

JANET AMMERMAN
California Bar # 113996
Federal Trade Commission
600 Pennsylvania Ave. NW
Room H286
Washington, D.C. 20580
Telephone: (202) 326-3145
Facsimile: (202) 326-3395
Email: jammerman1@ftc.gov

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

FEDERAL TRADE COMMISSION, Plaintiff, v. AUTOMATED ELECTRONIC CHECKING, INC., a Nevada corporation; JOHN P. LAWLESS, individually, and as an officer of Automated Electronic Checking, Inc; and KENNETH MARK TURVILLE, individually, and as an officer of Automated Electronic Checking, Inc., Defendants.	CV- COMPLAINT FOR INJUNCTIVE AND OTHER EQUITABLE RELIEF

Plaintiff, the Federal Trade Commission ("FTC" or "Commission"), for its Complaint alleges:

1. This case concerns the Defendants' practice of debiting the bank accounts of consumers for fraudulent and unauthorized charges, in violation of the Federal Trade Commission Act, 15 U.S.C. Section 45(a). The Defendants, acting as a payment processor on behalf of client merchants who were engaged in

fraud, used a relatively new payment mechanism that lacked systemic monitoring in order to debit money from consumer bank accounts, deduct Defendants' own fees, and transfer the remainder to said client merchants. Undaunted by glaring indicators that the transactions were induced by fraud or were unauthorized, Defendants continued to process such payments for years.

2. The FTC brings this action under Section 13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 53(b), to obtain permanent injunctive relief, rescission or reformation of contracts, restitution, the refund of monies paid, disgorgement of ill-gotten monies, and other equitable relief against Defendants for engaging in unfair acts or practices in connection with their processing of debits and charges to consumer financial accounts on behalf of Defendants' client merchants. Defendants' acts and practices violate Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

JURISDICTION AND VENUE

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

4. Venue in this District is proper under 15 U.S.C. § 53(b) and 28 U.S.C. §§ 1391(b) and (c).

PLAINTIFF

5. Plaintiff, the FTC, is an independent agency of the United States Government created by statute. 15 U.S.C. §§ 41-58. The FTC is charged, *inter alia*, with enforcement of Section 5(a)

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

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

DEFENDANTS

7. Defendant Automated Electronic Checking, Inc. ("AEC") was a Nevada corporation with its principal place of business at 4910 Mill Street, Reno, Nevada 89502. It was engaged in the business of providing payment processing services to merchants, including many who are considered "high-risk" by banks and the payment processing industry. AEC transacted business in this District. AEC dissolved its corporate status in March 2012.

8. Defendant John P. Lawless ("Lawless") was the CEO, Secretary, Treasurer and 45% owner of AEC. Individually or in concert with others, he has formulated, directed, controlled, has

authority to control, or has participated in the acts and practices set forth herein. He transacts or has transacted business in connection with the matters alleged herein in this District and throughout the United States.

10. AEC, Lawless, and Turville are hereinafter referred to collectively as "Defendants."

COMMERCE

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

DEFENDANTS' BUSINESS PRACTICES

Introduction

12. From at least 2007 through at least 2011, AEC has operated as a third-party payment processor ("payment processor"). As a payment processor, AEC has entered into contracts with merchants ("client merchants") in which AEC has agreed to process the exchange of money between the client merchant and the client merchant's customers.

13. In order to provide payment processing services, AEC entered into contractual relationships with one or more banks through which it agreed to transmit the transactions through the banking system. During the period from 2007 through 2011, AEC processed debits through at least four banks: (1) First Regional Bank in Century City, California; (2) Metro Phoenix Bank in

First Bank of Delaware in Wilmington, Delaware.

14. Several of AEC's client merchants have engaged in unfair and deceptive practices to obtain consumer financial account information, resulting in fraudulent and unauthorized debits to consumers' accounts.

15. AEC has played a critical role in its client merchants' unlawful business practices. It has provided its client merchants with access to the United States banking system, has controlled the procedures through which money is debited from consumers' bank accounts, and has disbursed consumer funds back to its client merchants.

16. AEC knew, or should have known, that its client merchants induced consumers to buy their products through fraudulent representations and routinely failed to obtain the consumers' authorization for debits to their accounts.

17. In some instances, AEC debited the bank accounts of consumers who had been misled regarding the nature of the product offered for sale. For example, many consumers believed they were applying for a credit line offered through one of AEC's client merchants, only to learn that instead, they had been enrolled in an online "shopping club" with hefty fees.

18. In many other instances, AEC debited the bank accounts of consumers who had never heard of AEC's client merchants, had never knowingly agreed to purchase any products or services from AEC's client merchants, and had not authorized a debit to their account. For example, AEC debited the bank account of Jacob A.

d) Christopher S. informed his bank that he did not authorize the charge and asked that the bank reverse the unauthorized debit. The bank informed him that he needed to file a report with the police, which he did.

e) Christopher S. gave a copy of the police report to his bank but the bank never refunded the charge to his account or the overdraft fee.

20. Tens of thousands of consumers have been harmed by AEC's business practices. While some consumers, often only after a great deal of effort, ultimately were able to obtain refunds for the fraudulently-induced and unauthorized debits, many were not. Also, many of the victimized consumers had insufficient funds in their bank accounts to cover the unauthorized AEC debits, resulting in overdraft charges for which few were reimbursed.

21. The impact of AEC's payment processing activities is widespread and has caused substantial injury to tens of thousands of consumers, many of whom can least afford to have funds taken from their accounts without authorization.

22. As set forth below, from at least 2007 to at least 2011, AEC has engaged in fraudulent and unauthorized debiting through the following means:

a) AEC has encouraged its client merchants to use a payment mechanism that is not subject to systemic monitoring;

b) AEC has processed payments for high-risk clients, through banks engaged in risky practices;

c) AEC has turned a blind eye to its client merchants' excessively high return rates;

d) AEC has instructed its client merchants on methods to avoid detection; and

e) AEC has ignored and failed to investigate consumer complaints.

23. AEC's unfair practices are exemplified in its relationship with its client merchants EdebitPay LLC and Platinum Online Group, as set forth in greater detail below.

AEC Encouraged its Client Merchants to Use
Remotely Created Payment Orders
To Avoid Systemic Monitoring

24. AEC's client merchants marketed and sold their products and services on websites or through telemarketing, without face-to-face contact with the consumer. AEC therefore offered payment processing services to merchants using payment methods that did not require a consumer's signature, including bank debits processed through the Automated Clearing House Network ("ACH transactions") and bank debits processed through remotely created payment orders ("RCPOs"). At issue in this complaint is the payment mechanism known as the RCPO.

25. Both ACH transactions and RCPOs result in money being withdrawn from (or deposited into) a bank account without the use of conventional physical checks. However, there are important differences between the two payment methods.

a) Instead of using paper to carry necessary transaction information, ACH transactions are transmitted between financial institutions through electronic data transmission using a batch processing, store-and-forward system called the ACH Network. Common examples are direct deposits of an employee's salary or automatic monthly debits to pay for a health club membership.

b) In contrast, an RCPO is a payment mechanism that is processed through the banking system much like a traditional paper check, even though it does not exist in paper form. An RCPO is an electronic image of a "virtual" check, created by the payment processor or merchant using the consumer's personal and financial account information. The image looks like a

s2

s

27. ACH transactions are the subject of regular oversight and scrutiny, as the National Automated Clearing House Association ("NACHA"), a private self-regulatory trade association, enforces a system of rules, monitoring, and penalties for noncompliance. Among other things, NACHA monitors the levels at which attempted ACH debits are returned by consumers or consumers' banks because high rates of returned transactions ("return rates") can be indicative of unlawful practices, such as unauthorized debiting of consumer accounts.

28. In contrast, the volume and rate of returned RCPO transactions are not subject to systemic monitoring by any centralized entity in the check clearing system. Largely because of the lack of systemic return rate monitoring, and because a consumer's actual signature is not required on an RCPO, RCPOs have become an attractive payment mechanism for merchants and processors engaged in unauthorized debiting and other unlawful practices.

29. AEC encouraged its client merchants to switch to RCPO processing because RCPOs are not subject to the same systemic monitoring and regulation as ACH transactions.

a) For example, in January 2008, AEC's principal Mark Turville notified one client merchant that "NACHA is going to a 1% threshold for unauthorized transactions starting 12-21-2007 and being enforced 3-21-2008." Turville urged the merchant to consider switching to RCPOs: "As you know our new [RCPO] product is now being used by most of our clients and does not have a 1%

restriction . . . .”

b) In October 2008, one of the banks processing debits for AEC notified AEC that it was concerned about the unauthorized return rates that one of its clients was generating for ACH transactions. The bank wrote, “Given these numbers and the fact that NACHA . . . has warned us and the fact that we are getting complaints already from consumers, it would be best that you put this client on [RCPO] for everything, no ACH at all.” AEC’s principal, Mark Turville, responded that AEC was “switching all the accounts under this client . . . to [RCPO] immediately.”

30. AEC’s client merchants generated extraordinarily high rates of returned RCPO transactions. Between 2007 and 2011, AEC processed RCPO bank debits to consumer accounts for merchants who generated total return rates of 50%, 60%, 70%, and even higher than 80%. AEC was aware of these return rates because it was notified by the processing bank every time a transaction it had processed was returned.

31. The total return rate reflects the percentage of all returned transactions (regardless of the return reason), out of the total number of attempted debits. Therefore, a greater than 50% total return rate means that for all consumer transactions processed on behalf of a given merchant, more than half the transactions were rejected by consumers or their banks.

32. Since at least 2007, AEC has used RCPOs to debit, or attempt to debit, millions of dollars from consumers’ bank accounts on behalf of its client merchants, even though consumers

and banks routinely rejected the transactions because they were unauthorized and fraudulent.

AEC's Clients' High Return Rates for
Not Authorized, Insufficient Funds, and Bad Account Information
Were Indicators of Possible Unauthorized Debiting

33. When a bank rejects an attempted debit to its account holder's account, the bank designates a reason for the rejection. Such reasons include "Not Authorized," "NSF" (or "insufficient funds"), and "Account Closed." As a payment processor, AEC was notified by the bank of the return reason for each transaction AEC processed that was returned.

34. The "Not Authorized" designation is used when a debit to a bank customer's account initially clears, but the consumer subsequently expressly notifies the bank that the debit was unauthorized.

35. Obviously, a high rate of transactions returned as "Not Authorized" puts the payment processor, such as AEC, on explicit notice that a high percentage of transactions were not authorized by the consumer.

36. However, high rates of returns in other return categories can also reflect fraudulent and unauthorized debiting.

a) For example, high rates of returns for insufficient funds, or "NSF," may also be indicators of unauthorized debiting. Consumers who are likely to have insufficient funds in their accounts do not commonly "authorize" merchants to debit their accounts, because these consumers know they will incur substantial overdraft charges imposed by the banks.

b) Similarly, high rates of returns due to account-number discrepancies may be a warning sign of fraud or unauthorized debiting. If a significant percentage of the merchant’s transactions are rejected because the consumer’s bank is unable to locate an account matching the information provided excessively high return rates, AEC failed to take reasonable steps to ensure that it was not engaging in fraudulent and unauthorized debiting on behalf of these client merchants.

AEC Matched High-Risk Clients
With High-Risk Banks

40. AEC's business has focused on client merchants who were considered to be "high-risk," in part because of the high rates at which their transactions were returned.

41. AEC's pricing structure has been such that the income earned by AEC from returned transactions was significantly higher than the income earned from merely processing a transaction that ultimately cleared. The more returned transactions generated by AEC's client merchants, the higher the return fees earned by AEC and its banks.

42. Despite the higher fees, many banks were reluctant to do business with "high-risk" merchants.

43. The few banks who were willing to do business with AEC and its "high-risk" client merchants were often engaged in risky practices themselves, and consequently found themselves in trouble with banking regulators. As a result, AEC was forced to move from bank to bank, constantly seeking out new places to process payments for its client merchants.

44. From 2008 through early 2010, AEC processed payments through First Regional Bank located in Century City, California.

45. However, in January 2010, First Regional Bank was shut down by the Federal Deposit Insurance Corporation ("FDIC"). This

followed charges by the FDIC that the bank was engaged in “unsafe or unsound banking practices.” The assets of First Regional Bank were sold to another bank, which decided it did not want to continue processing payments for AEC.

46. AEC was able to keep some of its client merchants by entering into an arrangement with another payment processor, CheckGateway, which had an ongoing relationship with Metro Phoenix Bank in Phoenix, Arizona. CheckGateway was not willing to accept all of AEC’s client merchants (it rejected EdebitPay LLC, among others), but for those it was willing to accept, AEC transmitted those clients’ transactions to CheckGateway, which, in turn, processed them through Metro Phoenix Bank. This relationship lasted from approximately February 2010 through November 2010.

47. Metro Phoenix Bank also attracted the attention of the FDIC, which ultimately charged that it had insufficient capital and was involved in unsound banking practices. In November 2010, Metro Phoenix Bank entered into a consent order with the FDIC and ceased all processing for AEC client merchants.

48. Meanwhile, AEC had located another payment processor through whom it was able to funnel transactions to yet a different bank. In late March 2010, AEC entered into an agreement with a payment processor called Elite Debit, which had a relationship with SunFirst Bank in St. George, Utah. AEC transmitted client merchants’ transactions to Elite Debit, which processed the transactions through SunFirst Bank.

49. In November 2010, SunFirst signed a Consent Order with the FDIC, in which it agreed to cease processing for Elite Debit and various other third party payment processors.

50. Shortly thereafter, the FTC sued Elite Debit. In announcing the lawsuit, the FTC said Elite Debit was part of "a far-reaching Internet enterprise that allegedly has made millions of dollars by luring consumers into 'trial' memberships for bogus government-grant and money-making schemes, and then repeatedly charging them monthly fees for these and other memberships that they never signed up for."

51. In November 2011, SunFirst Bank was seized by state regulators and the FDIC was appointed as receiver.

52. Meanwhile, AEC found another means of processing payments by establishing a relationship with First Bank of Delaware in Wilmington, Delaware. From approximately August 2010 to February 2011, AEC processed client merchants' transactions through that bank.

53. In addition to processing for AEC, First Bank of Delaware also processed for several other high-risk payment processors , including Landmark Clearing, Inc. In December 2011, First Bank of Delaware entered into a Consent Order with the FDIC in which it agreed to terminate all E-Payment Programs, including the processing of remotely-created checks and similar instruments. Also in December 2011, Landmark Clearing, Inc. entered into a Stipulated Final Order with the FTC to resolve charges of unauthorized debiting.

54. On November 19, 2012, First Bank of Delaware entered into a settlement with the U.S. Department of Justice, U.S. Attorney's Office for the Eastern District of Pennsylvania, which included a concurrent assessment of a civil money penalty of $15 million with the FDIC and the Financial Crimes Enforcement Network ("FinCEN"). In its civil complaint, the Department of Justice alleged that the bank violated the Financial Institutions Reform, Recovery and Enforcement Act ("FIRREA") by, among other things, debiting the bank accounts of consumer victims on behalf of fraudulent merchants and payment processors working in cahoots with such fraudulent merchants. On October 23, 2012, the bank's shareholders approved the bank's dissolution.

55. In February 2011, after repeatedly having been forced to cease processing with different banks and third party processors – and having failed to find others who would accept its client merchants – AEC suspended its payment processing operations.

AEC Instructed Its Client Merchants On Methods to Avoid Detection

56. Although it used banks willing to engage in risky practices, AEC recognized that the banks were under pressure from bank regulators and that AEC therefore needed to take additional steps to conceal its fraudulent and unauthorized debiting.

57. AEC recommended that its client merchants use various corporate names, dbas, customer service email addresses, and phone numbers, in order to conceal obvious signs of fraud that

would compel a bank to terminate the merchant.

58. In a November 2008 email, an AEC employee advised a client merchant:

> We feel it is very important that as soon as possible you spread out your traffic using different descriptors and or corp. names/DBA also please use different customer service emails and phone numbers. The best way to fly under the bank radar is to put no more than 10K transactions per month under one descriptor/company/DBA. We just had a very large client who lost processing due to complaints. . . . [A] bank will look at what they see of the same and say we have of lot of these this must be fraud. By spreading it around they do not see a lot of the same. It is very dangerous to grow if the traffic is not spread around under different companies/DBAs, descriptors, customer service contacts . . . our goal is to keep you up long term.

59. AEC also took steps to disguise warning signs by manipulating its client merchants' return rates for the "Not Authorized" category. Knowing that its banks paid particular attention to returns classified as "Not Authorized," AEC used various techniques to make its client merchants' high "Not Authorized" return rates seem lower than they actually were.

a) An excessively high percentage of AEC's RCPO returns were designated by consumers' banks as "Refer to Maker"

Business Bureau, or other regulatory or enforcement agencies about unauthorized debits to their bank accounts.

62. In numerous instances, consumers submitted their complaints about unauthorized debiting directly to AEC.

63. In numerous instances, consumers' banks requested that AEC provide evidence of consumer authorization to debit specific accounts.

64. Whenever consumer complaints came to its attention, AEC steadfastly refused to admit that they were valid. An egregious example of this occurred in 2009, when Bank of America informed AEC's bank, First Regional Bank, that hundreds of Bank of America's account holders had complained about unauthorized debits.

65. In a letter dated April 22, 2009, an official from Bank of America's Check Fraud Claims Department advised First Regional Bank that hundreds of Bank of America accounts continued to be debited by First Regional Bank's customers. "Since our last letter [in October 2008], the demand drafts [RCPOs] have increased . . . . Our customers are advising us that these transactions are not authorized. These transactions occur daily." The letter asked First Regional Bank to "do the right thing and make Bank of America's customers whole for the unauthorized transactions."

66. First Regional Bank turned to AEC, the processor responsible for many of these unauthorized debits, for a response. In an email to First Regional Bank dated April 23,

other financial services products, such as short-term loans. The prepaid cards were marketed with names such as “Elite Plus MasterCard” and “Sterling VISA.” These products were targeted at consumers who had difficulty getting credit. EdebitPay and Platinum marketed these products both on its own websites and on websites operated by third-party affiliate marketers.

74. AEC began processing RCPO transactions for EdebitPay in February 2008, just weeks after EdebitPay and its principals

down operations under the name EdebitPay, and to continue their operations using a company with a new name, Platinum Online Group. According to Cleveland, the primary reason for the name change was to "sidestep" the negative publicity associated with the name "EdebitPay" as a result of the FTC action.

79. AEC began processing RCPOs for Platinum in November 2009 and continued until February 2010.

80. When First Regional Bank terminated AEC as a payment processor in early 2010, AEC tried to find a new bank willing to contract with AEC to process payments for Platinum. After six months AEC was finally successful, and arranged to process payments for Platinum through Elite Debit with SunFirst Bank.

81. AEC resumed processing for Platinum for about two and a half months, finally terminating its processing for Platinum for good in November 2010, when SunFirst Bank was ordered to cease third-party processing.

82. Between November 2009 and November 2010, AEC processed more than $8 million in RCPO transactions for Platinum.

83. In total, from February 2008 to November 2010 (a time period spanning two years and nine months), AEC processed more than $49.8 million in RCPO transactions on behalf of EdebitPay and Platinum.

84. AEC knew or should have known that many of these transactions were fraudulent or unauthorized.

//

//

EdebitPay and Platinum's High Total Return Rates
Were a Warning Signal
of Fraudulent or Unauthorized Debiting

85. The most obvious evidence of EdebitPay and Platinum's fraudulent and unauthorized debiting was the astronomically high rate of returned transactions that these merchants generated.

86. EdebitPay and Platinum's total return rates, when compared with the 2011 average industry total return rates for ACH transactions nationwide, were shockingly high.

a) The average industry total return rate for ACH transactions in 2011 was 1.5 percent. (NACHA 2011 Return Rates; the NACHA average industry return rates were essentially identical from one year to the next during 2007 through 2011.)

b) In comparison, EdebitPay's total return rate was 85 percent for the transactions processed by AEC. This is over fifty times the average industry total return rate for ACH transactions.

c) Similarly, Platinum's total return rate was 86 percent, also over fifty times the average industry total return rate for ACH transactions.

87. The exceptionally large volume of returned transactions was a glaring sign that EdebitPay and Platinum were grossly out of sync with legitimate commerce.

88. The extremely high levels of returned transactions generated by EdebitPay and Platinum were evidence that they were attempting to debit consumer accounts with information obtained through fraudulent, deceptive, or unfair practices.

were, the “Not Authorized” return category was just the tip of the iceberg. Most of the thousands of consumers who called and emailed EdebitPay, complaining that they had never heard of it and did not know why their accounts had been debited, were not counted in the “Not Authorized” return statistics. These consumers included:

a) consumers who sought a refund from EdebitPay after their accounts were debited without their consent -- these were not counted as a “return” by the bank, because the debits were successfully processed,

b) consumers for whom the transaction was returned as “NSF,” and

c) consumers who tried to stop the unauthorized debiting by closing their account, resulting in a return for “Unable to Locate.”

“NSF” Returns

93. An excessively high percentage of AEC’s RCPO returns for EdebitPay and Platinum were categorized as NSF. These high NSF return rates, which vastly exceeded normal return rates for that category, were another red flag for unauthorized debiting.

(a) The ACH industry average for “NSF” returns was 1.04 percent of all ACH debit transactions in 2011. Rate for ACH Return Code R01, NACHA 2011 Return Rates.

(b) In comparison, EdebitPay’s “NSF” return rate was more than 59 percent .

(c) Platinum’s “NSF” return rate was more than 51 percent .

94. These NSF return rates made it abundantly clear that many consumers were unaware that their accounts were about to be debited. As one consumer wrote in an email to EdebitPay:

> There must be some kind of mistake, I do not want this service and did not order it. I applied for an auto loan online and now I have paid 3 overdraft charges for a service that I did not order. I don't know why my checking info went over to you guys. ... Please cancel this and please stop trying to withdraw money from my account.

"Bad Account" Returns

95. Similarly, an excessively high percentage of AEC's RCPO returns for EdebitPay and Platinum occurred due to account-number-discrepancy reasons.

(a) The ACH industry average for such returns totaled 0.35 percent of all ACH debit transactions in 2011. Combined Rate for ACH Return Codes R2, R03, R4, NACHA 2011 Return Rates.

(b) The return rate for EdebitPay due to "Account Closed," "Invalid Account," or "Unable to Locate" was more than 19 percent, or nearly 53 times higher than the ACH industry average.

(c) For Platinum, the return rate for these reasons was even higher – more than 23 percent.

96. These extraordinarily high return rates for "Not Authorized," "NSF," and "Bad Account" put AEC on notice that it was processing a large number of transactions that had not been

properly authorized.

AEC Knew that EdebitPay and Its Principals
Previously Had Been Sued by the FTC
and Were Subject to An Existing FTC Order

97. In addition to the bald data evincing unauthorized debits, other information in AEC's possession indicated that EdebitPay and Platinum and its principals posed a high risk of engaging in fraudulent practices.

98. The FTC filed a complaint on July 30, 2007 against EdebitPay and its principals Cleveland and Wilson, alleging, among other things, that EdebitPay engaged in deceptive marketing practices and debited consumers' bank accounts without their express informed consent, including consumers who had never applied for or requested the product EdebitPay was selling. The complaint also alleged that many consumers incurred NSF overdraft fees caused by the unauthorized debits.

99. On January 28, 2008, EdebitPay and its two principals, Cleveland and Wilson, settled with the FTC, agreeing to pay $2.2 million in consumer redress and agreeing to an order that prohibited them from, among other things, deceiving consumers or debiting consumers without obtaining their express informed consent.

100. In February 2008, when AEC began processing RCPO transactions for EdebitPay, AEC was aware of the FTC action and injunctive order against EdebitPay and its principals, Cleveland and Wilson.

//

AEC Knew or Should Have Known That EdebitPay Was Operating In Violation of the Consent Order

101. EdebitPay violated the 2008 FTC Stipulated Order during the time period that AEC processed its transactions.

102. On May 27, 2010, the FTC filed an action seeking to hold EdebitPay and its principals in contempt of the 2008 Order, alleging, among other things, that their online advertisements for a credit line were false and misleading. The Court agreed, and on February 3, 2011, the judge found EdebitPay and its principals, Cleveland and Wilson, in contempt, ordering them to pay $3.7 million in monetary sanctions.

contains copies of various website images advertising the Century Platinum "credit line," with precisely the same small font and obscure disclaimers that the Court found to be undeniably misleading.

105. Despite publicly-available information about the May 27, 2010 filing of the FTC action seeking to hold EdebitPay and its principals in contempt for violation of the 2008 Order, AEC actively sought to resume processing for them. On July 14, 2010, AEC principal Mark Turville sent an email to Wilson at EdebitPay saying, "We have some new banks online and I wanted to see if we could get some of your processing back."

106. In August 2010, AEC was able to resume processing payments for Wilson and Cleveland (under their new company name, Platinum) through Elite Debit and SunFirst Bank. AEC continued to process for Platinum until the FDIC ordered SunFirst Bank to terminate processing for third parties in November 2010.

AEC Knew or Should Have Known
That EdebitPay Marketed Its Products
on Payday-Loan Websites

107. A large percentage of EdebitPay's alleged sales of financial products occurred not on websites dedicated to such products, but on websites at which a consumer could apply for a short-term, high-interest loan or cash advance. Often such loans were to be repaid with the consumer's next paycheck (referred to as "payday loans"). These sites had names such as "Cash-In-1-Hour.com," "cashwiredfast.com," "easycashadvance.com," and "getyourpaydayadvance.com."

108. The payday loan websites presented an application form for a short-term loan or cash advance, which typically required the applicant to submit his or her name, address, telephone number, Social Security number, employment information, and bank account number.

109. Offers for additional products or services, or “upsells” (such as alleged credit repair services, identity theft protection, or the prepaid debit card offered by EdebitPay), would also appear on the payday loan website.

110. Once a consumer supplied his bank account information as part of the payday loan application, that bank account information could be used to debit the consumer’s account for an “upsell” product, whether or not the consumer knowingly authorized such a debit.

111. Based on statements of consumers, thousands of consumers who had provided personal information at a payday loan website were debited by AEC on behalf of EdebitPay, even though the consumers did not want or agree to purchase any “upsell” product and had no knowledge of who the merchant was or why their account was being debited.

112. In many instances, these consumers were not aware that their accounts were going to be debited until their bank notified them that a debit transaction had been attempted and returned for insufficient funds.

113. In other instances, the consumers happened to review their bank statements and noticed that money had been removed

from their account without their authorization. As consumer James K. of Duluth, Minnesota declared, "I had never heard of the company before. I never purchased any product from them, I did not authorize them to charge my account, and I do not know how they received my account information."

114. AEC either never asked for or ignored EdebitPay's customer service records, which revealed thousands of consumer complaints of unauthorized debiting, many involving payday loan websites.

AEC Took Active Steps to Conceal Warning Signs Regarding Platinum

115. AEC not only disregarded warning signs indicating fraud and unauthorized debiting in connection with EdebitPay and Platinum, but took active steps to conceal or disguise them.

116. For example, in order to obtain the approval of its banks to process transactions for Platinum, AEC submitted a merchant application form on behalf of Platinum despite knowing that it contained numerous misleading statements.

a) It is common for unscrupulous online merchants, particularly those who have been sued by the FTC or other regulatory bodies, to stop operating under their original business name and resume operations under a new name, in order to avoid the negative publicity associated with the original name. EdebitPay has freely admitted that this was the reason it created the entity "Platinum" in November 2009 and began operating under that name.

Consumers Were Harmed By AEC's Unauthorized Debiting

118. Consumer injury caused by AEC's unauthorized debiting practices has been substantial in at least three ways: (1) by debiting millions of dollars from consumers' bank accounts without consumer authorization; (2) by causing significant overdraft charges to consumers; and (3) by forcing consumers (and banks) to take the time and effort to reverse debits and, in certain instances, to close or change their accounts.

119. The debit transactions processed by AEC and returned for insufficient funds triggered thousands of dollars in overdraft charges to consumers. Thus, even when AEC was unable successfully to debit from consumers' accounts due to insufficient funds, many consumers still suffered harm. And with very few exceptions, neither AEC nor its client merchants reimbursed consumers for overdraft fees, and consumers' banks often refused to do so as well. Other consumers were forced to close their accounts in an effort to stop repeated unauthorized debit attempts. These consumers expended time and money in closing the old account and opening a new one, for which they were not reimbursed.

VIOLATIONS OF SECTION 5 OF THE FTC ACT

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

121. Acts or practices are unfair under Section 5 of the FTC Act if they cause or are likely to cause substantial injury

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

COUNT I

122. Defendants' acts or practices in processing fraudulent and unauthorized debit transactions to consumers' bank accounts, as described in paragraphs 12 - 119 above, have caused or are likely to cause substantial injury to consumers that is not reasonably avoidable by consumers themselves and that is not outweighed by countervailing benefits to consumers or competition.

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

CONSUMER INJURY

124. Defendants have caused consumers substantial monetary loss by causing funds to be debited from consumers' bank accounts on behalf of merchants engaged in deceptive, misleading, or unfair sales practices, which also resulted in other related consumer harm, such as incurring the costs of closing accounts, paying overdraft fees, opening new accounts, and ordering new checks. Consumers could not reasonably have avoided this injury. Defendants have been unjustly enriched as a result of their unlawful practices. Absent injunctive relief by this Court, Defendants are likely to continue to injure consumers, reap unjust enrichment, and harm the public interest.

disgorgement of ill-gotten [illegible];

D. Award Plaintiff the costs of bringing this [illegible]

[illegible]

General Counsel [illegible], Acting

[illegible]

Janet Ammerman
Michelle Chua
[illegible]
(202) 326-3248; mchua@ftc.gov (Chua);
[illegible]