Exhibit F

PREET BHARARA United States Attorney for the Southern District of New York

By: JEFFREY ALBERTS

Assistant United States Attorney

(212) 637-1038

9 MAG 2382

UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

TO BE FILED UNDER SEAL

ALL FUNDS ON DEPOSIT AT FIFTH THIRD : AFFIDAVIT IN SUPPORT BANK IN ACCOUNT NUMBERS 7431859508, OF SEIZURE WARRANTS HELD IN THE NAME OF VIABLE MARKETING CORP., AND ALL PROPERTY TRACEABLE THERETO;

_ _ _ _ _ X

: PURSUANT TO 18 U.S.C. §§ 981, 984 & 1955

ALL FUNDS ON DEPOSIT AT FIFTH THIRD : BANK IN ACCOUNT NUMBERS 7432618069, HELD IN THE NAME OF VIABLE MARKETING CORP., AND ALL PROPERTY TRACEABLE THERETO;

ALL FUNDS ON DEPOSIT AT BANK OF AMERICA, IN ACCOUNT NUMBERS 229006067857, HELD IN THE NAME OF VIABLE MARKETING CORP., AND ALL PROPERTY TRACEABLE THERETO; and

ALL FUNDS ON DEPOSIT AT BANK OF AMERICA, IN ACCOUNT NUMBERS 003678667131, HELD IN THE NAME OF EZO, LLC, AND ALL PROPERTY TRACEABLE THERETO;

Defendants-in-rem.

STATE OF NEW YORK)
COUNTY OF NEW YORK) ss: SOUTHERN DISTRICT OF NEW YORK)

REBECCA E. VASSILAKOS, being duly sworn, deposes and says:

- Investigation ("FBI") and have been so employed since December 2007. I am assigned to a squad that investigates organized criminal activity, including financial institution fraud and money laundering. I am familiar with the facts and circumstances set forth below from my personal participation in the investigation, my review of bank records and other documents, my conversations with civilian witnesses and other law enforcement officers, and my review of sworn affidavits of other law enforcement officers. Where the actions, statements, and conversations of others are recounted herein, they are recounted in substance and in part, unless otherwise indicated. Because this affidavit is for the limited purpose of establishing probable cause for a seizure warrant, it does not set forth every fact learned in the course of this investigation.
- 2. This affidavit is submitted in support of the Government's application for the issuance of warrants to seize and forfeit the following:
 - a. ALL FUNDS ON DEPOSIT AT FIFTH THIRD BANK IN ACCOUNT NUMBERS 7431859508, HELD IN THE NAME OF VIABLE MARKETING CORP. (the "FIFTH THIRD BANK VIABLE ACCOUNT 1"), AND ALL PROPERTY TRACEABLE THERETO;
 - b. ALL FUNDS ON DEPOSIT AT FIFTH THIRD BANK IN ACCOUNT NUMBERS 7432618069, HELD IN THE NAME

OF VIABLE MARKETING CORP. (the "FIFTH THIRD BANK VIABLE ACCOUNT 2"), AND ALL PROPERTY TRACEABLE THERETO;

- C. ALL FUNDS ON DEPOSIT AT BANK OF AMERICA, IN ACCOUNT NUMBERS 229006067857, HELD IN THE NAME OF VIABLE MARKETING CORP. (the "BANK OF AMERICA VIABLE ACCOUNT 1"), AND ALL PROPERTY TRACEABLE THERETO;
- d. ALL FUNDS ON DEPOSIT AT BANK OF AMERICA, IN ACCOUNT NUMBERS 003678667131, HELD IN THE NAME OF EZO, LLC, (the "BANK OF AMERICA EZO ACCOUNT 1") AND ALL PROPERTY TRACEABLE THERETO;

(collectively, the "Defendant Funds").

- 3. As set forth below, there is probable cause to believe that the Defendant Funds are property involved in actual or attempted money laundering transactions, or property traceable to such property, in violation of 18 U.S.C. § 1956(a). As such, the Defendant Funds are subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 984.
- that the Defendant Funds are property that constitute or are derived from proceeds traceable to the operation of an illegal gambling business, in violation of 18 U.S.C. § 1955, and the illegal transmission of gambling information, in violation of 18 U.S.C. § 1084, and property used in the operation of an illegal gambling business and commission of the gambling offense. As such, the Defendant Funds are subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(C), 984, and 1955(d).

BACKGROUND

- For approximately three years FBI agents have been investigating illegal internet gambling businesses which, although typically based offshore, predominantly serve players based in the United States. These gambling businesses offer "real money" casino games, poker, and sports betting to United States players, in violation of multiple federal criminal statutes including but not limited to 18 U.S.C. § 1084 (making it unlawful to use a wire in connection with placing a bet or wager), § 1955 (making it illegal to operate an illegal gambling business) and §§ 1956 and 1957 (money laundering). Although these gambling businesses are based offshore, the vast majority of their customers are in the United States. Consequently, these internet gambling businesses necessarily rely on the United States financial system to accept funds from online gamblers, transfer funds back to gamblers, and move funds between the United States bank accounts of their customers and the offshore accounts of the gambling businesses. And because the internet gambling is illegal in the United States, the gambling companies must, in most instances, deceive United States financial institutions about the nature of their accounts in the United States and the purposes of their financial transactions.
- 6. The internet gambling businesses rely on payment processors that use the Automated Clearing House system or "ACH

system" - both to obtain money from United States-based gamblers and to pay those gamblers seeking to withdraw funds from the gambling companies. The ACH system, which is administered by the Federal Reserve, allows for fast and efficient electronic funds transfers to and from individuals' checking accounts through "e-checks" or "electronic checks." External payment processors with access to the ACH system can "pull" money from individual consumer bank accounts (i.e. debit the consumer's account) and route it to gambling companies (typically based abroad) and "push" money from the gambling companies into individual checking accounts to pay winnings (i.e. credit the consumer's account). Typically, a gambler simply logs onto the web site of an internet gambling company and chooses "e-check" or some similarly described option and enters his or her United States bank account information to complete these transactions. However, because United States banks cannot lawfully process ACH payments relating to online gambling, the external payment processing companies must take steps to deceive financial institutions in order to induce them to allow such ACH processing. So, as is the case with credit card processing, external payment processors create phoney non-gambling internet businesses (complete with web pages, and in many cases corporate formalities) and represent to banks that they are processing on behalf of these businesses.

RELATED G.I. HOLDINGS SEIZURE WARRANT

- 7. On August 25, 2009, the Government sought a seizure warrant for the following property on the grounds that those funds (like the Defendant Funds) consist of property involved in actual or attempted money laundering transactions, or property traceable to such property, and consist of property that constitutes or is derived from proceeds traceable to the operation of an illegal gambling business, and the illegal transmission of gambling information, and property used in the operation of an illegal gambling business and commission of the gambling offense:
 - a. ALL FUNDS ON DEPOSIT AT CITY NATIONAL BANK IN ACCOUNT NUMBER 370117950, HELD IN THE NAME OF G.I. HOLDINGS, AND ALL PROPERTY TRACEABLE THERETO (the "City National G.I. Holdings Account");
 - b. ALL FUNDS ON DEPOSIT AT WELLS FARGO BANK IN ACCOUNT NUMBER 5383346862, HELD IN THE NAME OF G.I. HOLDINGS, AND ALL PROPERTY TRACEABLE THERETO (the "Wells Fargo G.I. Holdings Account");
 - C. ALL FUNDS ON DEPOSIT AT CITIBANK, N.A., IN ACCOUNT NUMBERS 203023239 AND 203118542, HELD IN THE NAME OF G.I. HOLDINGS, AND ALL PROPERTY TRACEABLE THERETO (the "Citibank G.I. Holdings Accounts");
 - d. ALL FUNDS ON DEPOSIT AT SERVICE 1ST BANK OF NEVADA IN ACCOUNT NUMBER 2020003792, HELD IN THE NAME OF G.I. HOLDINGS, AND ALL PROPERTY TRACEABLE THERETO (the "Service 1st G.I. Holdings Account"); and

e. ALL FUNDS ON DEPOSIT AT NEVADA COMMERCE BANK
IN ACCOUNT NUMBERS 0021002712 AND 0021002795,
HELD IN THE NAME OF G.I. HOLDINGS, AND ALL
PROPERTY TRACEABLE THERETO (the "Nevada
Commerce G.I. Holdings Accounts");

(Collectively, the "Seized G.I. Holdings Accounts")

- 8. In support of the application for a seizure warrant for the Seized G.I. Holdings Accounts, the Government submitted the Affidavit of FBI Special Agent Rebecca E. Vassilakos (the "Vassilakos G.I. Holdings Affidavit"), which is attached hereto as Exhibit 1 and incorporated by reference herein. On the basis of the Vassilakos G.I. Holdings Affidavit, the Honorable Ronald L. Ellis, United Stated Magistrate Judge, Southern District of New York, issued seizure warrants for the Seized G.I. Holdings Accounts, which are attached hereto as Exhibit 2. Judge Ellis ordered that the Vassilakos G.I. Holdings Affidavit must remain under seal until further order of the Court.
- 9. As discussed more fully in the Vassilakos G.I.
 Holdings Affidavit, in June and July 2009, G.I. Holdings was
 depositing hundreds of thousands of checks that G.I. Holdings
 printed, with G.I. Holdings as the payee and individuals as the
 payors. These checks generally were in the range of
 approximately \$15 to \$600, and generally were processed in
 batches of thousands of checks. The various Seized G.I. Holdings
 Accounts suffered from high chargeback rates as thousands or tens
 of thousands of payors disputed the payments.

- deposited into the G.I. Holdings accounts had "GREEN2YOURGREEN" in their memo lines; sometimes "GREEN2YOURGREEN" appeared by itself, but more often it appeared with a phone number and with the symbol "PS," "FT," or "UB." Based on my investigation, I believe that "PS," "FT," and "UB" stand, respectively, for "PokerStars," "Full Tilt Poker," and "Ultimate Bet," three of the largest online gambling operations in the world. Later, some of the Green2YourGreen checks replaced the codes "PS," "FT," and "UB" with "1" (or "one"), "2" (or "two") and "3" (or "three").
- at which it opened accounts that it was a payment processing company for various businesses other than online gambling businesses. G.I. Holdings represented to its banks that Green2YourGreen was a "multi-tiered" marketing firm that sold green or eco-friendly products.
- Holdings Affidavit, a cooperating witness (the "CW") who has previously provided reliable and corroborated information in connection with this investigation deposited money into online poker accounts at fulltiltpoker.com and pokerstars.com. Shortly thereafter, cancelled checks posted to the CW's bank account. The cancelled checks were a pre-printed check written to G.I. Holdings in the amount of the online deposits and were stamped as

deposited in the Seized G.I. Holdings Accounts. In at least one instance, after certain Seized G.I. Holdings Account were frozen, the CW received an email from the online poker website stating that deposits to the CW's online poker account had been delayed due to "an issue with one of our 3rd party processors."

13. In addition, overseas wires were sent from at least one of the Seized G.I. Holdings Accounts, including wires to Estonia, Cyprus, India, Latvia, Australia, Malta, and the Philippines.

RELATED JOHN SCOTT CLARK COMPLAINT

14. On or about June 24, 2009, a criminal complaint against John Scott Clark was filed under seal in the Southern District of New York, charging Clark with conspiracy to commit money laundering in violation of Title 18, United States Code, Section 1956(h), conspiracy to commit bank fraud in violation of Title 18, United States Code, Section 1349, and conspiracy to run an illegal gambling business and to accept a financial instrument for unlawful internet gambling, in violation of Title 18, United States Code, Section 371. The complaint in <u>United States</u> v. <u>John Scott Clark</u>, 09 Mag. 1488 (S.D.N.Y.) (the "Clark Complaint"), attached hereto as Exhibit 3, was based on the sworn deposition of Special Agent Roy Pollitt of the FBI. Based on the Clark Complaint the Honorable Henry B. Pitman, United States Magistrate

Judge, Southern District of New York, issued a warrant for Clark's arrest.

- established ACH processing accounts for a company located in Australia that provided ACH payment processing for multiple online gambling websites (the "Australian Gambling Processor") and processed hundreds of millions of dollars of ACH transactions for the Australian Gambling Processor. When opening at least some of these accounts, Clark misrepresented to the financial entity at which the account was held, sometimes ACH Processors, that the account would be used to process payday loans, when in fact they were used to process transactions for the Australian Gambling Processor.
- submitted to an ACH processor an application to perform payment processing for "Viable Processing Solutions," purportedly for processing payday loans. On this application, Elie was listed as the owner of Viable. Clark and Elie also represented to National Bank of California that the business of Viable Processing Solutions was payday loans. The ACH processor began processing ACH transactions for Viable Processing Solutions on or about September 16, 2008, and processed more than \$16 million in transactions over approximately five weeks through the National

Bank of California. Some of the transactions were from banks located in the Southern District of New York.

National Bank of California e-mailed two individuals at the ACH Processor, noting that a customer had attempted to return a \$100 ACH deposit made into the Viable bank account with the descriptor "increasedfunds.com." When the manager called the telephone number identified for "increasedfunds.com" he was referred to a customer support representative in Australia who stated that he worked for the Australian Gambling Processor.

FIFTH THIRD BANK VIABLE ACCOUNT 1

- 18. I have reviewed documents relating to the Fifth
 Third Bank Viable Account 1 obtained from Fifth Third Bank, and I
 have spoken with employees of Fifth Third Bank concerning Fifth
 Third Bank Viable Account 1. From that review of documents and
 discussion, I learned in substance and in part the following:
 - a. Chad Elie opened the Fifth Third Bank Viable

 Account 1 and is the signer on that account.
 - b. Fifth Third Bank Viable Account 1 was funded primarily through a high volume of pre-authorized and remotely drafted electronic checks made payable to INSTANTCS.COM, which is a name under which Viable Marketing Corp. does business. Most of these checks were for amounts lower than

- \$2,500. In August 2009, approximately 148,123 items were deposited to the account, totaling approximately \$14 million.
- c. Fifth Third Bank had a high rate of chargebacks for the Fifth Third Bank Viable Account 1. As of September 30, 2009, approximately 15,916 items were returned to the account for approximately \$4,611,000.
- d. Employees of Fifth Third Bank in the Bank

 Protections Group contacted at least two

 individuals who had checks issued from their

 accounts in the name of INSTANTCS.COM. One of

 these individuals had checks made out to both G.I.

 Holdings and INSTANTCS.COM. issued from the

 individual's account. Each of these individuals

 stated that he or she was an online gambler and

 that checks issued from their accounts could be

 related to online gambling.
- e. Employees of Fifth Third Bank in the Anti-Money
 Laundering Group also reviewed the accounts of two
 additional individuals who had checks issued from
 their accounts in the name of INSTANTCS.COM. Each
 of these individuals had checks made out to both
 G.I. Holdings and INSTANTCS.COM. issued from their

- accounts. One of the two accounts showed checks made out to G.I. Holdings deposited into one of the seized Citibank G.I. Holdings Accounts. The other account showed checks issued into the same seized account, as well as the seized City National G.I. Holdings Account and one of the seized Nevada Commerce G.I. Holdings Accounts.
- f. In September 2009, four wires were sent from Fifth Third Bank Viable Account 1 to an account located in the Phillippines, each ranging in value from approximately \$500,000 to approximately \$2 million. Later in September 2009, Fifth Third Bank placed a hold on the account.
- g. As of October 19, 2009 the account balance of Fifth Third Bank Viable Account 1 was approximately \$8,174,000.

FIFTH THIRD BANK VIABLE ACCOUNT 2

- 19. After Fifth Third Bank Viable Account 1 was put on hold, \$100,000 was transferred to Fifth Third Bank Viable Account 2 by Fifth Third Bank. Since that time the balance has declined to approximately \$40,000 due to chargebacks on the account.
- 20. Under Title 18, United States Code, Section 984, "any identical property found in the same place or account as the property involved in the offense that is the basis for the

forfeiture shall be subject to forfeiture" in "any forfeiture action in rem in which the subject property is . . . funds deposited in an account in a financial institution." 18 U.S.C. § 984. Accordingly, at least \$100,000 currently located in Fifth Third Bank Viable Account 1 is subject to forfeiture, which is greater than the current account balance.

BANK OF AMERICA ACCOUNTS

- 21. I have reviewed documents relating to Bank of America Viable Account 1 and Bank of America EZO Account 1 obtained from Bank of America, and I have spoken with an employee of Bank of America concerning Bank of America Viable Account 1 and Bank of America EZO Account 1. From that review of documents and discussion, I learned in substance and in part the following:
 - a. In May 2007, Chad Elie opened Bank of America

 Viable Account 1. Elie currently is a signer on

 that account.
 - b. In November 2008, a cashier's check in the amount of \$750,000 from a National Bank of California account held in the name of "Viable Processing Solutions," was deposited in the EZO Account 1 W
 - c. As of today, Bank of America Viable Account 1 has a balance of \$371,824.63.
 - d. Elie is a signer for Bank of America EZO Account1.

- e. In September 2008, five wires from an account at Zions First National Bank in the name of Desert Payment Systems (the "Desert Payment Systems Account") for an approximate total of \$170,000 and one wire of \$100,000 from an account at Zions First National Bank in the name of Digital Processing Solutions (the "Digital Processing Solutions Account") were made into Bank of America EZO Account 1.
- f. As of today, Bank of America EZO Account 1 has a balance of \$33,743.75.
- 22. I have spoken with an employee of Zions

 Bancorporation, the parent company of Zions First National Bank,

 concerning the Desert Payment Systems Account and the Digital

 Processing Solutions Account. From that review of documents and

 discussion, I learned in substance and in part the following:
 - a. Clark and/or five other individuals were signers on 200 to 250 accounts at Zions First National Bank, with Clark personally being a signer on most of them.
 - b. Zions Bancorporation analyzed the accounts on which Clark and/or five other individuals were signers, including the Desert Payment Systems Account and the Digital Processing Solutions

- Account. It found that money moved in a rapid, linear fashion between and among these accounts. It also found that transactions were made between the accounts in a layering fashion, which is a hallmark of money laundering transactions.
- c. Zions Bancorporation reviewed the various websites of Digital Processing Solutions LLC's clients and discovered the different websites were almost the same. The content was 95 percent similar, with photos being different.
- d. Based on its investigation, Zions Bancorporation closed the accounts on which Clark and/or five other individuals were signers between January and March 2009.
- 23. As described in further detail above and in the attached Clark Complaint, the ACH processor that performed payment processing for Viable Processing Solutions through National Bank of California ceased processing for the Viable Processing Solutions account in October 2008 after it was informed by a manager at National Bank of California that the phone number for the website listed on certain ACH transfer requests belonged to the Australian Gambling Processor.

- 24. I have spoken with John Scott Clark. From that discussion, I learned in substance and in part the following:
 - a. "Viable Processing" and "Desert Payment Systems" and "Digital" were companies created for the purpose of processing transactions for the Australian Gambling Processor.
 - b. Most transactions processed for the Australian Gambling Processor by companies that Clark controlled were done as part of the Australian Gambling Processor's business of processing transactions for internet poker companies.

STATUTORY AUTHORITY

- 25. The statutory provisions pursuant to which the contents of the Defendant Funds are subject to seizure and forfeiture are described below.
- 26. Title 18, United States Code, Section 981(a)(1)(A) subjects to forfeiture "[a]ny property, real or personal, involved in a transaction or attempted transaction in violation of . . . section 1956 . . . of this title, or any property traceable to such property."
- 27. Title 18, United States Code, Section 1956 provides, in pertinent part, that
 - (a)(2) Whoever transports, transmits, or transfers, or attempts to transport, transmit, or transfer a monetary instrument or funds from a place in the United States to

or through a place outside the United States or to a place in the United States from or through a place outside the United States--

(A) with the intent to promote the carrying on of specified unlawful activity

shall be quilty of a crime.

- 28. Title 18, United States Code, Section

 1956(c)(7)(A) provides that the term "specified unlawful
 activity" includes "any act or activity constituting an offense
 listed in section 1961(1) of this title". Included among the
 enumerated offenses in 18 U.S.C. § 1961(1) is 18 U.S.C. § 1955,
 which prohibits the operating of illegal gambling businesses, 18
 U.S.C. § 1084, and racketeering activity, which includes any act
 or threat involving gambling, which is chargeable under State law
 and punishable by imprisonment for more than one year.
- 29. Furthermore, 18 U.S.C. § 981(a)(1)(C) subjects to forfeiture:

Any property, real or personal, which constitutes or is derived from proceeds traceable to . . . any offense constituting 'specific unlawful activity' (as defined in section 1956(c)(7) of this title), or a conspiracy to commit such offense.

30. Again, as noted in paragraph 25, <u>supra</u>, 18 U.S.C. § 1956(c)(7)(A) provides that the term "specified unlawful activity" includes "any act or activity constituting an offense listed in section 1961(1) of this title," and § 1961(1) includes 18 U.S.C. §§ 1955 and 1084 among the enumerated offenses.

- 31. In addition, 18 U.S.C. § 1955 has its own forfeiture provision. Specifically, § 1955(d) provides that "[a]ny property, including money, used in violation of the provisions of this section may be seized and forfeited to the United States."
- 32. Furthermore, 18 U.S.C. § 984 provides, in relevant part, that:
 - (a) (1) In any forfeiture action in rem in which the subject property is . . . funds deposited in an account in a financial institution . . .
 - (A) it shall not be necessary for the Government to identify the specific property involved in the offense that is the basis for the forfeiture; and
 - (B) it shall not be a defense that the property involved in such an offense has been removed and replaced by identical property.
 - (2) Except as provided in subsection (b), any identical property found in the same place or account as the property involved in the offense that is the basis for the forfeiture shall be subject to forfeiture under this section.
 - (b) No action pursuant to this section to forfeit property not traceable directly to the offense that is the basis for the forfeiture may be commenced more than 1 year from the date of the offense.
- 33. Section 981(b)(1) of Title 18, United States Code, provides that any property subject to forfeiture to the United States under 18 U.S.C. § 981(a) may be seized by the Attorney

- General. Section 981(b)(2) provides that such a seizure may be made "pursuant to a warrant obtained in the same manner as provided for a search warrant under the Federal Rules of Criminal Procedure."
- 34. In addition, Section 981(b)(3) provides that, notwithstanding the provisions of Federal Rule of Criminal Procedure 41(a), a seizure warrant may be issued pursuant to Section 981(b) by a judicial officer in any district in which a forfeiture action against the property may be filed under Title 28, United States Code, Section 1355(b). Under Section 1355(b)(1)(A), a forfeiture action or proceeding may be brought in the district in which any of the acts or omissions giving rise to the forfeiture occurred.
- 35. Were this affidavit to be made public at this time, it would interfere with an ongoing criminal investigation into certain individuals engaged in the criminal business of online gambling and money laundering. Making the affidavit public also would interfere with the ability of law enforcement officers to locate and seize the proceeds of criminal online gambling businesses.
- 36. Should the court issue a seizure warrant on the basis of this affidavit, making that warrant publicly available before it is executed could interfere with the ability of law

enforcement officers to seize the Defendant Funds before they are dissipated.

CONCLUSION

37. For the foregoing reasons, I submit that there is probable cause to believe that the Defendant Funds are (a) monies involved in a money laundering transaction or attempted money laundering transaction, in violation of 18 U.S.C. §

1956(a)(2)(A); and (b) the proceeds of illegal internet gambling and property involved in illegal internet gambling, in violation of 18 U.S.C. § 1955. Accordingly, the Defendant Funds are subject to forfeiture to the United States of America pursuant to 18 U.S.C. §§ 981(a)(1)(A) and (C) and 1955, and I respectfully request that the Court issue a seizure warrant for the Defendant Funds, as described in paragraph 2, supra.

38. I also respectfully request that this Affidavit be sealed until further order of the Court and any warrant issued based on this Affidavit be sealed until it is executed, so as not to jeopardize the investigation of this matter.

Rebecca E. Vassilakos

Special Agent

Federal Bureau of Investigation

Sworn to before me this

OCT 2 6 2009

day of October, 2009:

HONORÁBLE FRANK MAAS

UNITÉD STATES MAGISTRATE JUDGE SOUTHERN DISTRICT OF NEW YORK

This Affidavit must remain under seal until further Order of the Court and the accompanying Seizure Warrant must remain under seal until it is executed.

SO ORDERED

OCT 2 6 2009

HONORABLE FRANK MAAS

UNITED STATES MAGISTRATE JUDGE SOUTHERN DISTRICT OF NEW YORK

OMITTED



Approved:

ARIC DEVITE BROWN / JONATHAN B. NEW

ARLO DEVLIN-BROWN / JONATHAY B. NE Assistant United States Attorneys

Before:

HONORABLE HENRY B. PITMAN

United States Magistrate Judge

Southern District of New York

9 MAG 1488

J IVELAND SEALED

UNITED STATES OF AMERICA

COMPLAINT

JOHN SCOTT CLARK,

- W -

18 U.S.C. §§ 371,

Violation of

1349, 1956(h)

Defendant.

COUNTY OF OFFENSE:

NEW YORK

_ _ _ _ _ _ _

SOUTHERN DISTRICT OF NEW YORK, ss.:

Roy Pollitt, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation and charges as follows:

COUNT ONE

- 1. From at least in or about February 2008 through at least in or about October 2008, in the Southern District of New York and elsewhere, JOHN SCOTT CLARK, the defendant, and others known and unknown, unlawfully, wilfully and knowingly did combine, conspire, confederate and agree together and with each other to violate Title 18, United States Code, Section 1956.
- JOHN SCOTT CLARK, the defendant, and other known and unknown, would and did transport, transmit, transfer and attempt to transport, transmit, and transfer a monetary instrument and funds from a place in the United States to or through a place outside the United States and to a place in the United States from or through a place outside the United States with intent to promote the carrying on of a specified unlawful activity, to wit, the operation of an illegal gambling business, in violation of Title 18, United States Code, Section 1956(a)(2)(A).

(18 U.S.C. § 1956(h))

COUNT TWO

3. From at least in or about February 2008 through at least in or about October 2008, in the Southern District of New

York and elsewhere, JOHN SCOTT CLARK, the defendant, and others known and unknown, unlawfully, willfully, and knowingly did combine, conspire, confederate, and agree together and with each other to commit an offense under Chapter 63 of Title 18, United States Code, to wit, a violation of Title 18, United States Code, Section 1344.

4. It was a part and an object of the conspiracy that JOHN SCOTT CLARK, the defendant, and others known and unknown, unlawfully, willfully, and knowingly would and did execute and attempt to execute a scheme and artifice to defraud a financial institution, the deposits of which were then insured by the Federal Deposit Insurance Corporation, to wit, Comerica Bank and the National Bank of California, and to obtain the moneys, funds, credits, assets, securities, and other property owned by and under the custody and control of, such financial institution, by means of false and fraudulent pretenses, representations and promises, in violation of Title 18, United States Code, Section 1344.

(18 U.S.C. § 1349).

COUNT THREE

- 5. From in or about February 2008 through at least in or about October 2008, in the Southern District of New York, and elsewhere JOHN SCOTT CLARK, the defendant, and others known and unknown, unlawfully, willfully, and knowingly did combine, conspire, confederate, and agree together and with each other to commit an offense against the United States, to wit, violations of Title 18, United States Code, Section 1955 and Title 31, United States Code, Sections 5363 and 5366.
- 6. It was a part and an object of the conspiracy that JOHN SCOTT CLARK, the defendant, and others known and unknown, unlawfully, willfully, and knowingly would and did conduct, finance, manage, supervise, direct, and own all and part of an illegal gambling business, namely a business that engaged in and facilitated online poker, in violation of New York State Penal Law Sections 225.00 and 225.05, and which business involved five and more persons who conducted, financed, managed, supervised, directed, and owned all and part of such business, and which business had been and remained in substantially continuous operation for a period in excess of thirty days and had gross revenues of \$2,000 in a single day, in violation of Title 18, United States Code, Section 1955.
- 7. It was further a part and an object of the conspiracy that JOHN SCOTT CLARK, the defendant, and others known and unknown, unlawfully, willfully, and knowingly would, with persons engaged in the business of betting and wagering, knowingly accept, in connection with the participation of another

person in unlawful internet gambling, to wit, gambling in violation of New York Penal Law Sections 225.00 and 225.05, an electronic fund transfer and the proceeds of an electronic fund transfer from and on behalf of such other person, in violation of Title 31 United States Code, Sections 5363 and 5366.

OVERT ACT

- 8. In furtherance of the conspiracy and to effect the illegal objects thereof, the following overt act, among others, was committed in the Southern District of New York:
- a. In or about May 2008, CLARK and other co-conspirators not named as defendants herein represented to an Automated Clearing House ("ACH") processor that they would be processing ACH payday lending transactions when in fact they intended to process internet gambling transactions, including in the Southern District of New York.

(18 U.S.C. § 371).

The basis for deponent's knowledge and for the foregoing charges are, in part, as follows:

- 9. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed for over twelve years. I am assigned to a squad that investigates organized crime, including "white collar" organized crime involving financial crime and money laundering. For approximately the past three years, I have served as one of the FBI agents primarily responsible for an investigation into illegal internet gambling businesses. In connection with this investigation, I have interviewed dozens of witnesses, including senior employees of internet gambling businesses and of payment processing companies that serve these businesses. I have also reviewed documents provided by the above sources, as well as other documents, such as bank records reflecting financial transactions relating to internet gambling.
- set forth below from my personal participation in the investigation, my review of bank records and other documents, and my conversations with civilian witnesses and other law enforcement officers, including the sources referenced in paragraph nine, above. Where the actions, statements, and conversations of others are recounted herein, they are recounted in substance and in part, unless otherwise indicated. Because this affidavit is for the limited purpose of establishing probable cause an arrest warrant, it does not set forth every fact learned in the course of this investigation.

Background

- I know from my involvement in this investigation that, beginning the late 1990s, various businesses - most of which were located outside of the United States - began offering various forms of "real money" online gambling over the internet to customers in the United States and around the world. The vast majority of users of these gambling websites were gamblers located in the United States. These websites offered a variety of games to bet on, ranging from sporting events to poker to casino games. These websites continued to operate notwithstanding warnings from the Department of Justice ("DOJ") that the operation of an internet gambling business violated multiple federal criminal laws, including but not limited to 18 U.S.C. §§ 1084, 1952 and 1955, and in spite of the federal prosecution of off-shore gambling businesses since at least in or about 1998, as in the case of United States v. Cohen, 260 F.3d 68 (2d Cir. 2001).2
- 12. In October 2006, the Unlawful Internet Gambling Enforcement Act ("UIGEA"), 31 U.S.C. § 5361, et seq., was signed into law. The UIGEA makes it a crime for persons "engaged in the business of betting or wagering" to "knowingly accept" credit cards, electronic fund transfers, checks and other financial instruments in connection with unlawful internet gambling. 31 U.S.C. §§ 5363, 5366. Also in 2006 both before and after the

4

¹ For example, in 2003, DOJ restated its position on internet gambling in a letter to United States broadcast organizations signed by them Deputy Assistant Attorney General John G. Malcolm. Malcolm wrote: "Notwithstanding their frequent claims of legitimacy, Internet gambling and offshore sportsbook operations that accept bets from customers in the United States violate Sections 1084, 1952, and 1955 of 18 of the United States Code, each of which is a Class E felony. Additionally, pursuant to Title 18, United States Code, Section 2, any person or entity who aids or abets in the commission of any of the above-listed offenses is punishable as a principal violator of those statutes. The Department of Justice is responsible for enforcing these statutes and we reserve the right to prosecute violators of the law."

Jay Cohen, the founder of World Sports Exchange, was convicted by a jury of conspiracy to violate the Wire Wager Act, 18 U.S.C. 1084(a), and seven substantive counts of violating, and aiding and abetting violations of, the Wire Wager Act, in connection with his operation of World Sports Exchange (WSEX). WSEX, located on the island of Antigua in the Caribbean, targeted customers in the United States through the placement of ads on the radio, in newspapers, and on television. Customers were invited to bet on American sporting events either by ringing a toll-free telephone number or by placing bets over the Internet. WSEX's activities in New York were also enjoined in an action brought by the New York Attorney General. N.Y. v. World Interactive Gaming Corp., 714 N.Y.S.2d 844, 848, 850-52 (N.Y.Sup.Ct. 1999). In granting the injunction, the court held: "The act of entering the bet and transmitting the information from New York via the Internet is adequate to constitute gambling activity within New York state," and that "the Wire Act, Travel Act and Wagering Paraphernalia Act all apply despite the fact that the betting instructions are transmitted from outside the United States over the Internet."

enactment of the UIGEA, and in reliance on federal statutes in effect prior to the passage of the UIGEA³ - DOJ brought several enforcement actions relating to internet gambling, including the arrest of the founder of BETONSPORTS, in July 2006 (who has since pled guilty), and the arrests in January 2007 of the founders of NETeller PLC, a on-line "e-wallet" that was primarily used by United States gamblers to transfer funds to and from internet gambling websites, including websites offering gambling on poker games exclusively.

13. Following the enactment of the UIGEA and the DOJ enforcement actions described above, several large industry leading publicly traded corporations that offered online gambling to United States residents, stopped doing business in the United States. However, other privately held online gambling companies — which were either already offshore, or relocated offshore following the passage of the UIGEA — continued to market their games in the United States and to accept payments from United States customers.

Payment Processing For Offshore Internet Gambling Companies

- 14. Although illegal internet gambling companies keep their computer servers, management and support staff offshore, they must rely on the United States financial system both to obtain money from gamblers and to pay those gamblers who wish to withdraw funds from the online gambling companies. However, because virtually all significant United States financial institutions refuse to handle financial transactions related to internet_gambling, the offshore internet_gambling_companies_and___ the payment processors who serve them must, as a matter of course, deceive United States financial institutions in order to conduct these transactions. Based on my review of records from several internet gambling companies, and interviews with numerous executives for such companies, billions of dollars each year are transferred to and from United States bank accounts to offshore internet gambling companies through transactions disguised as non-gambling related.
- 15. I and other FBI agents have spoken at length, and on multiple occasions, with three individuals who previously worked for leading internet poker companies and who had significant responsibility for obtaining payment processing solutions for these companies. These individuals ("Poker Processor 1", "Poker Processor 2" and "Poker Processor 3,"

³ The UIGEA had no effect on pre-existing gambling laws: "No provision of this subchapter shall be construed as altering, limiting, or extending any Federal or State law or Tribal-State compact prohibiting, permitting, or regulating gambling within the United States." 31 U.S.C. § 5361(b).

collectively, the "Senior Poker Processors") have provided information that has been corroborated by each other, by documents, and by other sources, and has proven to be reliable. According to the Senior Poker Processors, internet gambling companies are able to move gambling funds into and out of the United States through conduct designed to deceive United State banks. Specifically, according to the Senior Poker Processors, as corroborated by my review of financial and conversations with representatives of financial institutions:

- At present, the leading internet gambling companies rely in part on credit cards to obtain funds from United States customers. Mastercard and Visa require that these poker companies, through the banks serving them, apply a specific transaction code to credit card charges to fund the poker accounts - "7995" - so that the member banks who issue the credit cards to United States customers know that the transaction is online gambling-related and can determine whether or not the bank will allow their cardholders to use their credit cards for internet gambling transactions. Virtually all United States issuing banks block their cardholders from using their credit on "7995" coded gambling transactions. As a result, the major online gambling companies utilize external payment processors who help them trick United States issuing banks into treating the transactions as non-gambling. The external payment processors create dummy corporations nominally providing non-gambling services (such as online web stores selling various merchandise), build phoney web sites for these dummy corporations (so that, if a bank employee checks, the company will seem legitimate), and make arrangements with a bank (almost always offshore) to assign a non-7995 code to charges by these dummy corporations. The Senior Poker Processors have indicated that when a consumer pays by credit card on one of these gambling sites, the site will inform the customer of the name of the dummy non-gambling merchant that will appear on his or her credit card statement, a fact that I have confirmed by speaking with multiple gamblers (and reviewing screenshots - i.e. printouts taken from the computer screen - of their gambling activity) who have used credit cards to fund their online gaming accounts.
- b. Online gambling companies also rely on external payment processors that use the Automated Clearing House system or "ACH system" both to obtain money from United States-based gamblers and to pay those gamblers seeking to withdraw funds from the gambling companies. The ACH system, which is administered by

⁴ Poker Processor 1 has been offered a non-prosecution agreement by the United States Attorney's Office for the Southern District of New York (the "Office"). Poker Processor 2 has provided information pursuant to a grant of immunity. Poker Processor 3 has voluntarily provided information as part of discussions with the Office about the disposition of potential criminal charges against Poker Processor 3.

the Federal Reserve, allows for fast and efficient electronic funds transfers to and from individuals' checking accounts through "e-checks" or "electronic checks." External payment processors with access to the ACH system can "pull"money from individual consumer bank accounts (i.e. debit the consumer's account) and route it to gambling companies (typically based abroad) and "push" money from the gambling companies into individual checking accounts to pay winnings (i.e. credit the consumer's account). Typically, a gambler simply logs onto the web site of an internet gambling company and chooses "e-check" or some similarly described option and enters his or her United States bank account information to complete these transactions. However, because United States banks cannot lawfully process ACH payments relating to online gambling, the external payment processing companies must take steps to deceive financial institutions in order to induce them to allow such ACH processing. So, as is the case with credit card processing, external payment processors create phoney non-gambling internet businesses (complete with web pages, and in many cases corporate formalities) and represent to banks that they are processing on behalf of these businesses.

c. Off-shore internet gambling companies also need to deceive banks in order to settle gambling transactions with gamblers who wish to cash out their positions - i.e. withdraw their gambling "winnings" or, even if they have lost money, withdraw what remains of the funds initially deposited with the internet gambling company. The most cost-effective way to promptly pay gamblers in the United States is to mail checks drawn on bank accounts located in the United States. Therefore, offshore internet gambling companies maintain accounts in United States banks holding substantial funds. The offshore internet gambling companies attempt to disguise their connections to these United States bank accounts - in large part because of fear of seizure by law enforcement authorities - by opening accounts through external payment processors and using account holders with generic sounding names not associated with gambling. The external payment processors opening these accounts typically tell United States banks that checks will be issued from the accounts in connection with the operation of a non-gambling business, such as the issuance of consumer rebate checks.

Examples Of Deceptive ACH Transactions

16. The fact that internet gambling companies use deceptive methods in their ACH processing has been corroborated by those who have made ACH deposits on gambling websites. For example, I have spoken to several gamblers about their ACH deposits in February 2009 into accounts controlled by the leading online poker website serving the United States market ("Poker Company 1"). The information these gamblers have provided has been supported by documents that I have reviewed, including

screenshots of the Poker Company 1 website, e-mails from the online gambling companies to the gamblers, and bank statements. All of the gamblers' deposits and subsequent transactions were made in New York City, including in the Southern District of New York. This information and these documents show the following:

"ONESHOPCENTER"

- a. On one date in February 2009, 6 Gambler 1 made a deposit into his/her Poker Company 1 account via "e-check," through the ACH system. After making the deposit, Poker Company 1 sent Gambler 1 an e-mail stating that "this transaction will appear on your bank statement as ONESHOPCENTER (or an abbreviated version). On a second date in February 2009, Gambler 1 made an additional deposit and received essentially the same message from Poker Company 1.
- b. According to bank records, Gambler 1's payments to Poker Company 1 were "batched" through the ACH system to an account maintained at a bank in Arizona (the "Arizona Bank"), through which tens of millions of dollars were transferred via the ACH system between January and May of 2009, and through which more than \$50 million was ultimately transferred outside the United States. The "descriptor" associated with both transactions on the bank records identified the merchant as "ONESHOPCENTER."
- "www.oneshopcenter.com" that appears, at first blush, to be a legitimate website offering clothing and jewelry for sale. In fact, a representative of the Arizona Bank stated that she checked several of the websites referenced in the ACH descriptors and was satisfied that the merchant was real. In fact, however, the website is simply a false front for Poker Company 1. I know this, for among other reasons, because on or about March 3, 2009 an associate of Gambler 1's sent an e-mail to "billing@oneshopcenter.com" stating that s/he had placed an order for a silver necklace but that his/her confirmation notice had said to send a check for payment for the necklace without any

New York criminal law defines gambling to include staking something of value on a game "in which the outcome depends in a material degree upon an element of chance." New York Penal Law § 225. It is well established in New York that poker, while having some element of skill, depends on chance to a "material degree" and therefore constitutes gambling. See, e.g., People v. Turner 165 Misc.2d 222, 223-224, 629 N.Y.S.2d 661, 662 (N.Y.City Crim.Ct. 1995) (collecting cases).

⁶ I am aware of the exact dates and amounts associated with the transactions involving Gambler 1 and Gambler 2 described herein, but have omitted such dates in this complaint so as to protect the identities of these individuals.

indication as to where the payment should be sent. Approximately one hour later, "Manfred," a "Poker Company 1 Cashier Specialist," writing from the e-mail address "support@Poker Company 1.com", responded, "I do not quite understand your email. Please elaborate on your request." The associate of Gambler I responded again that s/he simply needed to know where to send the check for the necklace. A few hours later, "Diana," another "Poker Company 1 Cashier Specialist," e-mailed back: "Note that you are contacting Poker Company 1 support, we are an Online Poker company, visit us at "www.Poker Company 1.com." "Diana" did not address the request about how to pay for the necklace.

"MYGOLFLOCATION"

- d. On a date in February 2009 Gambler 2 made a deposit into his/her Poker Company 1 account via "e-check". After making the deposit, Poker Company 1 sent Gambler 2 an e-mail stating that "this transaction will appear on your bank statement as MYGOLFLOCATION(or an abbreviated version). The "descriptor" associated with this transaction Gambler 2's bank statement identified the merchant as "MYGOLFLOCATION."
- e. There was also a website accessible via the internet at "www.mygolflocation.com", which appeared to be in the business of selling golf equipment. In fact, however, the "mygolflocation.com" website is simply a false front for Poker Company 1. I know this, for among other reasons, because on or about March 18, 2009 an individual e-mailed "billing@mygolflocation.com" and stated "You guys may want to know that there is a problem with your web site. I saw a travel putter I wanted to get as a gift to someone but the check out form doesn't work." Approximately one and a half hours later, "Haydee," writing from "Poker Company 1 Payment Services" and using the e-mail address "paymentservices@Poker Company 1.com" wrote back, "We have been contacted by our echeck processor regarding a charge made to your checking account. Please be so kind and respond if you have an open account with Poker Company 1."

The Australian ACH Processing Channel and JOHN SCOTT CLARK

17. Poker Processor 3, who previously worked as a senior payment processor for a major internet poker website, has informed me that a company located in Australia provides ACH payment processing for multiple online gambling websites (the "Australian Gambling Processor"), and previously provided ACH processing for Poker Company 1 and its chief United States-facing competitor ("Poker Company 2") until it failed to pay those poker websites millions of dollars. Poker Processor 3 further informed me that the Australian Gambling Processor, like other ACH processors, used false merchants names and phoney websites in order to deceive United States banks into believing that the ACH

transactions that they were processing were for some purpose other than gambling. Poker Processor 3's statements have been corroborated by, among other things, information from a bank in the United States which refused to process transactions linked to the Australian Gambling Processor after receiving reports that the company was linked to internet gambling. Additionally, according to published reports, Poker Company 2 has filed a lawsuit against the Australian Gambling Processor in Australia seeking to collect millions of dollars owed to it.

- 18. Because the Australian Gambling Processor is based in Australia, and because the ACH system requires access to United States bank accounts to process ACH transactions, the Australian Gambling Processor has had to rely on individuals in the United States to set up ACH processing accounts for gambling transactions. For the reasons set forth below, I know that JOHN SCOTT CLARK, the defendant, has established ACH processing accounts for the Australian Gambling Processor and is otherwise associated with that company. Specifically:
- a. From speaking to another FBI agent who interviewed a representative of a Florida bank (the "Florida Bank"), and who reviewed Florida Bank records, I know that from February 2008 through July 2008, CLARK processed more than \$700,000,000 of ACH transactions for the Australian Gambling Processor through an account he was a signer on at the Florida Bank. The Florida Bank representative indicated that the Florida Bank stopped processing the Australian Gambling Processor transactions because, despite repeated requests from the bank representative, neither CLARK nor representatives of the Australian Gambling Processor could identify the purpose of the ACH transactions or provide any "proof of authorization" for the transactions (essentially, an ACH record showing that the individual had authorized the ACH withdrawal from his or her bank account on behalf of a particular merchant).
- b. According to public records CLARK is associated with more than 100 corporate entities, many of which are linked to Quasar Corporate Services, Inc., of which CLARK is President. Many of CLARK's entities overlap with Australian Gambling Processor entities in that they either (i) share similar names or (ii) share identical domain name registrants. Additionally, according to a representative of a building management company, an employee of Quasar ("Clark Associate 1") leased an apartment in a Las Vegas apartment building as a "corporate rental" and then provided the space to the founder and owner of the Australian Gambling Processor. An employee of a company linked to Clark Associate 1 also sponsored United States visas for several employees of the Australian Gambling Processor.
- c. One of CLARK's primary business banks, located in Utah (the "Utah Bank") has closed CLARK's business accounts after

learning that they were associated with internet gambling and money laundering. Another FBI agent has spoken to a representative of the Utah Bank, who indicated that CLARK previously maintained between approximately 200 to 250 bank accounts with the Utah Bank in various, similar sounding names, and on behalf of numerous companies with virtually identical websites. The Utah Bank representative further stated that money was frequently transferred between and among CLARK's accounts at the Utah Bank without any business purpose ascertainable to the Utah Bank, and that more than \$150 million was ultimately transferred to offshore accounts. In early 2009 the Utah Bank discovered that some of CLARK's accounts had been transferring more than \$10 million in large, whole-dollar transactions to a bank account linked to an IRS seizure of a gambling processing company. The Utah Bank ultimately terminated CLARK's accounts.

CLARK'S Fraudulent ACH Processing Through ACH Processor 1 & Comerica Bank

19. "ACH Processor 1" is a service provider that contracts with merchants to provide them with ACH processing services. ACH Processor 1 processes these transactions at accounts in multiple banks, including Comerica Bank, which is insured by the FDIC. ACH Processor 1's agreement with Comerica Bank, which I have seen, provided that ACH Processor 1 could only process transactions for certain lawful activities, and specifically excluded online gaming. Since 2007, ACH Processor 1 has been cooperating with the Government in connection with this online gaming investigation."

20. I have reviewed documents obtained from ACH Processor 1 and spoken to both the owner of ACH Processor 1 (the "ACH Processor 1 Owner") and the Risk Manager for ACH Processor 1 ("the Risk Manager"), regarding payment processing ACH Processor 1 engaged in on behalf of JOHN SCOTT CLARK, the defendant, through one of CLARK's companies. Based on my conversations with the ACH Processor 1 Owner, the Risk Manager, and a review of ACH Processor 1 documents, I am aware that CLARK sought and obtained an agreement with ACH Processor 1 to provide ACH processing services for what CLARK claimed was a payday loan business. Specifically:

Prior to its cooperation, however, ACH Processor 1 provided substantial ACH processing for NETeller PLC. Although customers could theoretically use NETeller's e-wallet for nongambling purposes, NETeller's e-wallet was in fact overwhelmingly used for gambling. In January 2007, millions of dollars of NETeller PLC funds were seized, including approximately forty-six million dollars held in bank accounts by ACH Processor 1, in connection with the arrest of two NETeller PLC founders.

- In approximately May 2008, CLARK submitted an application to ACH Processor 1 on behalf of "Draftlink LLC," representing in the application - and in statements CLARK made to the Risk Manager - that Draftlink, which CLARK said he owned, was in the business of processing "e-check" payments from individuals who wanted to use e-checks to repay money owed for payday loans. Specifically, according to CLARK, DraftLink LLC offered payday loans over the internet and then collected repayments of those loans electronically, via the ACH system. CLARK sought ACH Processor 1's services in obtaining a bank account through which Draftlink would be able to process the "payday loan" repayments and ACH Processor 1's services in processing the ACH transactions in that bank account through the ACH network. According to Poker Processor 3, who spoke to another FBI Agent on this subject, external payment processors serving the gambling industry sometimes disquise their ACH debits from gamblers' accounts by claiming they are transactions for payday lenders.
- b. After performing some initial due diligence on CLARK and reviewing the web site for Draftlink which, on its face, appeared to be a payday loan website, albeit one not presently functioning ACH Processor l agreed to process transactions for CLARK through an account at Comerica Bank. The agreement initially provided that ACH Processor l would hold the first \$6,000,000 of incoming e-check payments from the individuals repaying their alleged loans as a reserve against chargebacks (payments back to the debited consumer account where the account lacked sufficient funds, or where the consumer disputes the charge) and other problems.
- 21. From conversations with the ACH Processor 1 Owner, the Risk Manager, and my review of ACH Processor 1 documents, I learned that in approximately June 2008 ACH Processor 1 began processing transactions for DraftLink LLC through a Comerica Bank account. This included processing ACH debits from bank accounts located in the Southern District of New York. Shortly after it started processing these transactions, however, ACH Processor 1 learned that Draftlink was not processing "payday loan" repayments as JOHN SCOTT CLARK, the defendant, had represented, but was instead processing illegal gambling transactions. ACH Processor 1 came to this conclusion based on the following information:
- a. After approximately one week of processing, the Risk Manager noted that many of the payments from United States customers for DraftLink LLC were in amounts of hundreds of dollars, and, in numerous cases, the same customers would make deposits several days in a row. ACH Processor 1 had processed payments for other payday lenders before and, in the experience of ACH Processor 1, true repayments of payday loans were typically for smaller dollar amounts and were made at regular periodic intervals (such as weekly) and not several days in a

- b. The Risk Manager looked at the web sites for the supposed "payday loan" services that CLARK and his associates had provided to ACH Processor 1 and learned that the sites did not actually enable an individual to obtain or repay a payday loan and, instead, appeared to be inoperative. When ACH Processor 1 asked representatives of DraftLink LLC, to provide "proof of authorization" for a sampling of the transactions that is, screen shots or some other proof that the customer had authorized DraftLink LLC to make the debit on a payday loan website, and proof of the purpose of the debit DraftLink LLC was unwilling to do so.
- c. The Risk Manager then checked some of the names of the individuals whose accounts were debited through DraftLink LLC and found that several of these individuals had previously been customers of NETeller PLC an "e-wallet" used predominantly for gambling. A further, more comprehensive, study by ACH Processor 1 revealed that approximately 35% of the U.S. bank accounts making supposed "payday" loan payments to Draftlink LLC through ACH Processor 1 previously had been used to fund e-wallet accounts with NETeller PLC.
- 22. On or about July 8, 2008, ACH Processor 1 stopped processing transactions for Draftlink and informed the FBI that the Draftlink account appeared to be used to fund online gambling transactions. The Risk Manager then informed JOHN SCOTT CLARK, the defendant, and his associates, that ACH Processor 1 would stop processing for Draftlink and hold onto the funds in Draftlink's account at Comerica Bank (by then, approximately \$3 million) while it reviewed the transactions. While neither the Risk Manager nor anyone else at ACH Processor 1 told CLARK or his associates that the freeze was related to internet gambling, two of CLARK's associates - Clark Associate 1 (previously identified in paragraph 18b) and Clark Associate 2 - asked the Risk Manager if the bank suspected the transactions were related to internet gambling. Another Clark Associate (Clark Associate 3) informed the Risk Manager that Draftlink had "inadvertently" processed ACH transactions to load debit cards out of the account rather than payday loans.
- 23. JOHN SCOTT CLARK, the defendant, and his associates refused to accept ACH Processor 1's decision to stop processing Draftlink's transactions and to hold onto approximately \$3 million dollars in the Comerica Bank account, and demanded that the ACH Processor 1 Owner and the Risk Manager repay CLARK immediately, notwithstanding the fact that under Draftlink's agreement with ACH Processor 1, ACH Processor 1 had up to two years' to return the majority of the funds if suspicious transactions were identified in the processing account. The Risk Manager and the ACH Processor 1 Owner told CLARK and his

associates that the money could not be returned because the bank had put a hold on the funds while awaiting proof that the transactions were valid. Clark Associate 1 then called the Risk Manager and stated that he would "kill anyone who took their money" and further announced that they would come to ACH Processor 1's offices the following day.

24. In September, 2008 I spoke to one of the individuals whose checking account was debited by "Draftlink" through ACH Processor 1 and s/he stated that the transaction had been to fund his/her internet gambling account at either Poker Company 1 or Poker Company 2.

CLARK'S Fraudulent Processing Through ACH Processor 2 & The National Bank of California

- 25. In July, 2008 around the time that JOHN SCOTT CLARK, the defendant, encountered difficulties processing transactions through ACH Processor 1 CLARK sought to obtain ACH processing services from "ACH Processor 2" for what he claimed was "payday loan" processing. I have spoken to representatives of ACH Processor 2 and National Bank of California (which is insured by the FDIC), and reviewed documents provided by these sources. From these sources, I know the following:
- a. On or about July 1, 2008, CLARK submitted an application to ACH Processor 2 for ACH Processor 2 to perform payment processing on behalf of a company called "Viable Processing Solutions". ("Viable")., which, CLARK claimed, was in the business of processing payday loans. Although CLARK guaranteed the processing account, the owner of Viable was listed as Clark Associate 4. ACH Processor 2 began processing ACH transactions for Viable on or about September 16, 2008, and processed more than \$16 million in transactions over approximately five weeks through the National Bank of California. Some of the transactions were from bank accounts located in the Southern District of New York.

On or about September 9, 2008, a United States Magistrate Judge issued an order directing that the funds held for Draftlink LLC, which by then had been transferred to Bank of the West, be seized as proceeds of illegal gambling.

⁹ On or about March 26, 2007, ACH Processor 2 entered into a non-prosecution agreement with the United States Attorney's Office for the Southern District of New York concerning ACH Processor 2's processing of internet gambling transactions for NETeller PLC.

The Australian Gambling Processor has filed a lawsuit in the Middle District of Florida against Clark Associate 4 in which the Australian Gambling Processor has alleged that Clark Associate 4 stole \$4 million from one of Viable Marketing's bank accounts.

- On or about September 23, 2008, a manager from National Bank of California e-mailed two individuals at ACH Processor 2, noting that a customer had attempted to return a \$100 ACH deposit made into the Viable bank account with the descriptor "increasedfunds.com." When the manager called the telephone number identified for "increasedfunds.com" he was referred to a customer support representative in Australia who stated that he worked for the Australian Gambling Processor. As described in paragraph 17 above, the Australian Gambling Processor is a payment processor serving the internet gambling ACH Processor 2 relayed these concerns to Clark industry. Associate 1, who initially responded in an e-mail that this was simply the customer service center for Viable. In another e-mail of that same day, drafted by Clark Associate 3 and copied to CLARK, Clark Associate 3 apologized for the "confusion" and claimed that the transactions actually were not for payday loans but were for "debit card loads for general e-commerce." From speaking to Poker Processor 3, I know that ACH processors serving the internet gambling industry sometimes disquise gambling transactions as involving the loading of debit cards.
- c. Based on the above, ACH Processor 2 ceased processing for the Viable account in October 2008. Since that time, ACH Processor 2 has conducted a preliminary analysis showing a significant overlap between bank accounts used by NETeller's e-wallet customers and bank accounts debited by Viable through ACH transactions. Also, after National Bank of California closed the Viable bank account, the bank received a letter from an attorney who stated that he represented the Australian Gambling Processor and that the Australian Gambling Processor was entitled, by assignment, to collect Viable funds held by National Bank of California.

WHEREFORE, deponent prays that an arrest warrant be issued for JOHN SCOTT CLARK, the defendant, and that he be arrested and imprisoned or bailed as the case may be.

ROY POLLITT SPECIAL AGENT

FEDERAL BUREAU OF INVESTIGATION

Sworn to before me this 24th day of June 2009

HONORABLE HENRY B. PITMAN UNITED STATES MAGISTRATE JUDGE SOUTHERN DISTRICT OF NEW YORK