

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLORADO**

Civil Action No. 1:18-cv-

**KAZMIERA FRAZIER AND  
MATTIE WALKER**, individually and  
on behalf of all others similarly situated,

Plaintiffs,

v.

**THE WESTERN UNION  
COMPANY, WESTERN  
UNION FINANCIAL  
SERVICES, INC., HIKMET  
ERSEK, and Various “Doe”  
Defendants, Including Western  
Union Officers, Directors, and  
Agents,**

Defendants.

---

**CLASS ACTION COMPLAINT AND JURY DEMAND**

---

**TABLE OF CONTENTS**

**I. INTRODUCTION..... 3**

**II. JURISDICTION AND VENUE ..... 6**

**III. PARTIES..... 7**

**A. Plaintiffs ..... 7**

**B. Defendants ..... 8**

**IV. FACTUAL ALLEGATIONS..... 9**

**A. Western Union Operates and Controls a Global Money Transfer System ..... 9**

**B. Defendants Have Long Been Aware that the Western Union Money Transfer System Has Been Regularly Used to Defraud Innocent Customers ..... 12**

**C. Defendants Were Part of the Scheme to Defraud ..... 15**

**D. The Amount of Actual Fraud is Significantly Higher than What Was Reported in, and Subject to, the DPA..... 29**

**E. Equitable Tolling..... 29**

**V. CLASS ACTION ALLEGATIONS..... 34**

**VI. CLAIMS ALLEGED..... 37**

**FIRST CLAIM FOR RELIEF ..... 37**

**Violations of 18 U.S.C. § 1962(c) and (d) ..... 37**

**SECOND CLAIM FOR RELIEF ..... 40**

**Violations of 18 U.S.C. § 1962(b) and (d)..... 40**

**THIRD CLAIM FOR RELIEF ..... 42**

**Violations of Colo. Rev. Stat. Ann. § 18-17-104(3) and (4)..... 42**

**FOURTH CLAIM FOR RELIEF ..... 45**

**Violations of Colo. Rev. Stat. Ann. § 18-17-104(2) and (4)..... 45**

**FIFTH CLAIM FOR RELIEF ..... 46**

**Violations of Colo. Rev. Stat. § 18-4-405..... 46**

**SIXTH CLAIM FOR RELIEF..... 48**

**Negligence ..... 48**

**SEVENTH CLAIM FOR RELIEF ..... 49**

**Unjust Enrichment..... 49**

**EIGHTH CLAIM FOR RELIEF ..... 50**

**Conversion ..... 50**

**VII. JURY DEMAND ..... 51**

**VIII. REQUEST FOR RELIEF ..... 51**

Plaintiffs Kazmiera Frazier and Mattie Walker (collectively, “Plaintiffs”) bring this Complaint, individually and on behalf of the other members of the below-defined class they seek to represent (the “Class”) against Defendants, The Western Union Company, Western Union Financial Services, Inc., Hikmet Ersek, and various Doe Defendants, including Western Union officers, directors, managers, employees, and agents (collectively “Defendants,” unless otherwise identified), for violations of the Organized Crime Control Act of 1970, Pub. L. No. 91-452, Title IX, “Racketeer Influenced and Corrupt Organizations Act” (“RICO”) (codified at 18 U.S.C. §§ 1961-1968), violations of Colorado Organized Crime Control Act (“COCCA”), violations of Colorado’s theft statute, negligence, unjust enrichment, and conversion. The allegations set forth herein are based upon personal knowledge as to matters concerning Plaintiffs and their own acts and upon information and belief as to all other matters. The allegations that are not based on Plaintiffs’ personal knowledge result from Plaintiffs’ counsel’s investigation.

## **I. INTRODUCTION**

1. The Western Union Company (“Western Union” or the “Company”), along with various of its officers, directors, managers, employees, and agents, has admitted to rampant fraud, beginning as early as 2004, cheating its customers out of hundreds of millions of dollars.

2. On January 19, 2017, the United States Department of Justice (“DOJ”) announced a Deferred Prosecution Agreement (the “DPA”) with Western Union, and the United States Federal Trade Commission filed a complaint against Western Union (the “FTC Complaint”). These documents provided detailed facts confirming that Western Union and certain of its officers, directors, managers, employees, and agents, since at least as early as 2004, defrauded

Western Union customers out of hundreds of millions of dollars through the Western Union Money Transfer System.<sup>1</sup>

3. The facts revealed in the DPA and the FTC Complaint show that Defendants were not only aware that third-party fraudsters (hereinafter, “Fraudsters”) such as con artists and Internet scammers, routinely used the Western Union Money Transfer System to facilitate their scams, but that Defendants, for the purpose of lining their own pockets from the fees associated with fraudulent transactions, were essential actors in an overarching scheme to defraud its customers—including Plaintiffs and the other Class members—through the Western Union Money Transfer System operated by Defendant Western Union Financial Services, Inc. (“WUFSI”).

4. Defendants decided that they would not take adequate steps to prevent fraud, which would have included terminating agents known to be complicit with Fraudsters; rather, Defendants resolved that they would continue using the Western Union Money Transfer System to defraud innocent customers—including Plaintiffs and the other Class members—all for the sake of corporate profits.

5. In January 2018, Western Union entered into a Consent Order with the New York State Department of Financial Services (the “New York Consent Order”) that revealed further facts showing that various senior Western Union executives purposefully and knowingly perpetuated wire fraud.<sup>2</sup>

6. Plaintiffs and each of the other Class members were victims of Western Union’s wire fraud, as described in more detail below. Plaintiffs each contacted Western Union for

---

<sup>1</sup> To ensure accuracy, significant portions of the DPA and the FTC Complaint are paraphrased and used verbatim herein. True and correct copies of the DPA and FTC Complaint are attached hereto as Exhibits A and B.

<sup>2</sup> A true and correct copy of the New York Consent Order is attached hereto as Exhibit C.

assistance after they were defrauded through Western Union. In each instance, Western Union misled them by asserting that the Company had nothing to do with the fraud and there was nothing more that the Company could do for Plaintiffs. Due to Western Union's misrepresentations, Plaintiffs were ignorant of Western Union's involvement in the scheme to defraud through the Western Union Money Transfer System, and, with no way of identifying or locating the Fraudsters, Plaintiffs had exhausted any possible diligence they could perform into recovering their losses.

7. The facts showing Western Union's involvement in the systemic scheme to defraud innocent consumers were unknown—and could not have been known—until no earlier than January 19, 2017, when the DPA and FTC Complaint became public, and revealed the nature of Defendants' actions. The facts included within the DPA and FTC Complaint all came from confidential, internal Western Union documents that were not available to Plaintiffs and the other Class members.

8. Neither Plaintiffs nor the other Class members were ever privy to the facts or Western Union documents that served as a basis for the facts, admissions, and allegations set forth in the DPA, the FTC Complaint, and the New York Consent Order.

9. Due to the DOJ and FTC investigations, Western Union agreed to forfeit \$586 million and make the funds available to individuals who were defrauded through the Company from at least 2004 to 2017.

10. As is evident from the DPA, however, this \$586 million is insufficient to cover the damages of every person who was defrauded through the Company from 2004 to 2017. Moreover, Western Union was not given any release from civil RICO liability through either the DOJ and FTC settlements, or the New York Consent Order. Now that the true nature of

Defendants' involvement in their losses has been revealed, Plaintiffs and the other Class members are entitled to seek and obtain a full recovery of the amounts that they lost, and the amounts available under the federal and state RICO statutes asserted herein.

11. By this Complaint, Plaintiffs seek legal and equitable relief for themselves and the other Class members, in the manner set forth herein, based on the facts and criminal violations that Western Union has already *admitted* are true and correct.

## II. JURISDICTION AND VENUE

12. This Court has jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The matter in controversy, exclusive of interest and costs, exceeds the sum or value of \$5,000,000,<sup>3</sup> and is a class action in which there are at least one hundred Class members and Class members are citizens of states different from Western Union. Further, more than two-thirds of the Class members reside in states other than the states in which Western Union is a citizen. Plaintiffs are both citizens of the State of Georgia. Western Union is a citizen of Colorado and is registered to do business in every state in the United States.

13. This Court also has jurisdiction over this matter under 28 U.S.C. § 1331, and 18 U.S.C. §§ 1961, 1962, and 1964.

14. This Court has personal jurisdiction over Defendants, and venue is proper, under 18 U.S.C. § 1965 because Western Union transacts affairs in this District, and such jurisdiction serves the interests of justice, including the avoidance of multiple trials, unnecessary costs, excessive burden on witnesses, and the possibility of inconsistent verdicts.

15. Under 28 U.S.C. § 1367, this Court may exercise supplemental jurisdiction over the state law claims alleged herein because each of those claims is derived from a common

---

<sup>3</sup> In determining whether the \$5 million amount in controversy requirement of 28 U.S.C. § 1332(d)(2) is met, Class members' claims are aggregated. 28 U.S.C. § 1332(d)(6).

nucleus of operative facts and are such that Plaintiffs ordinarily would expect to try them in one judicial proceeding.

### III. PARTIES

#### A. *Plaintiffs*

16. Kazmiera Frazier is currently a resident of Warner Robins, Georgia. In 2005, while living in New Jersey, she was defrauded through a Western Union location in Newark, New Jersey.

17. Ms. Frazier was fraudulently notified over the telephone that she had qualified for a Pell Grant, and needed to wire \$175 through Western Union as a processing fee. She wired those funds through a Western Union location in Newark, New Jersey. After wiring the \$175, the Fraudster who falsely promised the Pell Grant then told Ms. Frazier that she needed to wire additional funds in order to receive the Pell Grant. At that point, Ms. Frazier realized that she was possibly the victim of a scam.

18. Upon that realization, Ms. Frazier promptly contacted Western Union and requested that it stop the transfer of her \$175 wire. Western Union told Ms. Frazier that it was too late, that Western Union couldn't do anything to help her, and that the problem was not Western Union's responsibility, because the scam was perpetrated by a third party. Ms. Frazier had no reasonable way of locating and holding the Fraudster accountable. Ms. Frazier did not know, and had no way of knowing, that Western Union was complicit in, or had recklessly or negligently enabled, the fraud.

19. Ms. Frazier was never directly notified that she could be reimbursed as part of the DPA, and has not been reimbursed as part of the DPA.

20. Mattie Walker is a resident of Macon, Georgia. In 2005, while living in Florida, Ms. Walker was defrauded through Western Union in Fernandina Beach, Florida.

21. Ms. Walker read a Craigslist advertisement for a job as a “secret shopper.” The purported job required her to report on the customer service of various businesses. After an initial assignment to review the service of a Wal-Mart, Ms. Walker was told to review a Western Union. The Fraudster behind the purported “secret shopper” job sent Ms. Walker a check for \$2,400 and told her to wire that same amount back to them through Western Union. The Fraudsters stopped payment on their check before the funds could reach Ms. Walker’s account. But Ms. Walker had already wired \$2,400 through a Western Union in Fernandina Beach, Florida. Upon realizing that payment had been stopped on the check that the Fraudsters had sent to her, Ms. Walker recognized that she was possibly the victim of a scam.

22. Upon that realization, Ms. Walker promptly contacted Western Union and asked that it stop the transfer of her \$2,400 wire. Western Union told Ms. Walker that it was too late, that Western Union couldn’t do anything to help her, and that the problem was not Western Union’s responsibility, because the scam was perpetrated by a third-party. Ms. Walker had no reasonable way of locating and holding the Fraudster accountable. Ms. Frazier did not know, and had no way of knowing, that Western Union was complicit in, or had recklessly or negligently enabled, the fraud.

23. Ms. Walker was never directly notified that she could be reimbursed as part of the DPA, and has not been reimbursed as part of the DPA.

**B. *Defendants***

24. The Western Union Company, is a Delaware corporation with its principal place of business located in Englewood, Colorado.

25. Western Union Financial Services, Inc. (“WUFSP”) is a Delaware corporation with its principal place of business located in Englewood, Colorado.



26. Hikmet Ersek has been the Chief Executive Officer of Western Union since 2010. He is an individual residing in the State of Colorado.

27. The “Doe” Defendants are yet-to-be-identified officers, directors, managers, employees, and agents of Western Union. They will be specifically identified during the course of discovery in this case.

#### **IV. FACTUAL ALLEGATIONS**

##### ***A. Western Union Operates and Controls a Global Money Transfer System***

28. Western Union is a financial institution and one of the largest money services businesses in the world. Western Union employs approximately 10,000 individuals worldwide.

29. In 2016, Western Union reported total revenues of \$5.4 billion, and completed 791 million transactions in over 200 countries, including more than \$80 billion in principal between consumers.

30. Western Union transmits and converts money. It earns revenue by charging its customers a fee based on the money transfer amount and the destination location

31. In order to conduct its money transfer business, Western Union is registered with the Financial Crimes Enforcement Network (“FinCEN”), and subject to its requirements and duties.

32. Western Union’s money transfer business is based on its “Money Transfer System,” which it operates and controls.

33. Western Union’s Money Transfer System is an electronic network, which uses interstate and foreign wires to complete money transfers. Consumers transmit money around the world using Western Union’s Money Transfer System.

34. All Western Union money transfers flow through the same global Money Transfer System.

35. WUFSI operates a network of approximately 550,000 agent locations in 200 countries and territories worldwide. As a part of the required anti-money laundering program, WUFSI was required to take reasonable steps to guard against the flow of illicit funds. In January 2017, WUFSI was fined by Financial Crimes Enforcement Network (“FinCEN”) for violating this requirement by failing to conduct adequate due diligence. Consequently, certain agent locations and outlets that WUFSI suspected were involved in fraud and money laundering were able to continue to use WUFSI’s money transfer system to facilitate their illicit activity.

36. “Western Union Agents” (or “Agents”) are generally independent individuals or entities that own and/or operate Western Union Agent locations pursuant to a contract with Western Union. These Agents are authorized to offer Western Union’s money transfers to consumers.

37. To send money through Western Union, consumers go to a Western Union Agent and provide the Agent with the sender and payee names, the transfer amount, and the location where the money is to be sent. Consumers also provide the Agent with the funds necessary to cover the transfer amount and the fee charged by Western Union.

38. To receive money through Western Union, the payee must typically appear in person at a Western Union Agent location and provide the Agent with identifying information, as well as the name of the sender and the expected transfer amount. To complete the transfer to the payee, the paying Agent transmits the payee’s information to the Western Union Money Transfer system via international or interstate wire.

39. Western Union’s contracts with its Agents require its Agents to comply with all applicable laws, including anti-money laundering laws.

40. Western Union's contracts further provide Western Union with the right to immediately suspend or terminate Agents and Agent locations. Western Union has the right to do so unilaterally and anywhere in the world for a variety of reasons, including compliance reasons.

41. Agents are required to keep records for all transactions, provide them to Western Union upon request, and cooperate with any audit or review by Western Union.

42. Western Union's contracts also provide Western Union with the right to inspect and audit its Agents' books and records to monitor compliance with the agreement, applicable law, and Western Union's policies.

43. Western Union pays Agents a commission for money transfers. It also provides bonuses and additional money to Agents for increased transaction volume.

44. Agents sometimes have sub-agents ("Sub-agents") that carry out money transfers using the Western Union Money Transfer System. Western Union's agreements with its Agents give Western Union the right to suspend and terminate Sub-agents.

45. Western Union has the ability to refuse or cancel any money transfer through its Money Transfer System.

46. Once Western Union's Agents have paid out the funds, Western Union's policy typically is that the sender cannot obtain a refund from Western Union of either the amount transferred or the money transfer fee, even if the sender was a victim of fraud or the money transfer was paid out to someone other than the intended recipient. The policy even applies if the Western Union Agent was complicit in the fraud, engaged in suspicious activity, or failed to follow Western Union's policies and procedures when processing the money transfer.

**B. *Defendants Have Long Been Aware that the Western Union Money Transfer System Has Been Regularly Used to Defraud Innocent Customers***

47. On its website, Western Union states: “Smart People Fall For Scams Every Day: Con artists use good people like you, and good money transfer companies like Western Union, to steal money.”

48. Indeed, Western Union provided an essential service to Fraudsters by permitting them access to Western Union’s Money Transfer System. Exploiting this service, Fraudsters have stolen, and continue to steal, millions of dollars from innocent consumers. This fraud has also generated substantial revenue for Western Union and its Agents, in the form of transaction fees and foreign currency exchange fees.

49. Since at least January 2004, Defendants have been aware, based on hundreds of thousands of complaints, internal reports and records, and repeated warnings from government agencies around the world, that Fraudsters have regularly used Western Union’s Money Transfer System to fraudulently obtain funds from their victims.

50. Western Union has conducted reviews and investigations, and has generated reports, related to consumer fraud involving its Money Transfer System. This information, available only to Western Union, showed that the Company was aware of high levels of consumer fraud involving Western Union Agents.

51. Defendants were aware of specific Agents and Sub-agents that were the subject of abnormally high levels of fraud complaints; and were further aware knew that many of its Agent locations with high fraud had: (a) violated Western Union’s anti-fraud policies and procedures; (b) engaged in suspicious activities; and (c) been complicit, or likely complicit, in fraud.

52. Defendants were aware of Agent locations—particularly overseas Agent locations—that processed high levels of fraud transfers from U.S. victims, including certain Agent locations that Defendants suspected were complicit in the fraud scheme.

53. Western Union identified corrupt Western Union Agents through various means, including internal Consumer Fraud Reports, transaction monitoring, and other reports generated by Western Union analysts reviewing transactions that highlighted Agent locations exhibiting evidence of complicity in fraud.

54. Defendants also knew that certain Agent locations were actively engaged in fraud using Western Union’s Money Transfer System because some of those locations were prosecuted for their criminal activity. For example, between 2001 and 2012, 28 Western Union Agent owners, operators, or employees were charged in the U.S. District Court for the Middle District of Pennsylvania for their participation in fraud or money laundering using Western Union’s Money Transfer System.

55. In addition, for many years, law enforcement agencies in the United States and throughout the world warned Western Union that its Money Transfer System was being used to perpetrate consumer fraud and that Western Union was not adequately addressing the problem.

56. In or around 2002, multiple state Attorneys General issued subpoenas to Western Union in conjunction with their investigations of the use of Western Union’s Money Transfer System by fraudulent telemarketers.

57. In correspondence dated October 1, 2002, the Vermont Attorney General’s Office informed Western Union about alarming statistics regarding telemarketers using Western Union’s Money Transfer System for fraudulent schemes.

58. Since at least June 2011, the Minnesota Attorney General's Office has warned Western Union's President and Chief Executive Officer, Defendant Hikmet Ersek, that "each year thousands of consumers are defrauded through use of your company's services," and that "[g]iven your firm's apparently continuing inability or unwillingness to detect and prevent such wire transfer fraud, it would seem appropriate to" issue refunds to consumers. In response, Western Union typically has refused to issue any refunds to the victims after the funds were transferred.

59. In October 2011, multiple state Attorneys General issued subpoenas to Western Union in connection with investigations of fraudulent telemarketers' use of Western Union's Money Transfer System. The Vermont subpoena stated that it had "reason to believe that Western Union has provided substantial assistance to fraudulent telemarketers in the form of access to its money transfer system, despite knowing, or consciously avoiding knowing, of the fraud, in violation of the Vermont Consumer Fraud Act, 9 V.S.A. § 2453(a)."

60. Further, Defendants were aware of systemic fraud because some (but not all) defrauded consumers contacted Western Union to report on, and inquire about, fraud-induced money transfer issues.

61. When victims of fraud through Western Union's Money Transfer System complained to Western Union, it recorded these complaints and generated Consumer Fraud Reports ("CFRs"). The CFRs contained detailed information about the victims, the transactions, and the Agent locations that paid the transfers. Western Union maintained a database of all CFRs.

62. Western Union’s CFR database revealed rampant fraud perpetrated through its Money Transfer System. According to Western Union’s own confidential records, which it concealed from the public, and were only made public through the DPA and the FTC Complaint:

a. Between January 1, 2004, and August 29, 2015, Western Union received at least 550,928 complaints about fraud-induced money transfers, totaling at least \$632,721,044. Over 80% of the complaints in the database were from U.S. consumers. The average individual consumer fraud loss was approximately \$1,148. This is more than three times the amount of Western Union’s average money transfer for the years 2010 through 2014—approximately \$346—and more than seven times the amount of Western Union’s median money transfer for the same period;

b. Since at least 2004, the United States has been the top country for fraud payouts and has generated over three times the number of complaints as the next highest country. Over \$128.2 million in reported fraud has been paid out in the United States since 2010, and Western Union has received more than 34,000 fraud complaints about transactions totaling over \$21.2 million since 2014; and

c. Western Union received additional complaints, which were not recorded in the database, including at least 8,497 complaints in 2005 regarding fraud-induced money transfers, which totaled at least \$14,478,365.

63. When a victim reported fraud to Western Union in October 2012, she was told by a Western Union employee that she was “wasting [her] time” reporting the fraud because “there are thousands of these complaints laying on the desk and nothing gets done.”

***C. Defendants Were Part of the Scheme to Defraud***

64. With knowledge of rampant ongoing fraud within the Money Transfer System, Defendants sent wires as part of scheme to defraud across interstate and international borders.

Defendants purposefully facilitated Fraudsters' actions, including by failing to take steps to prevent Fraudsters from engaging in fraud, so as to benefit from the fees the Fraudsters generated for Western Union.

65. At the most blatant level, certain Agents and Sub-agents knowingly engaged with Fraudsters to steal from innocent customers. Corrupt Agents would (a) conceal the true identities of the fraudsters; (b) fail properly to collect and record all of recipients' IDs or biological information, and (c) knowingly record obviously false information such as false addresses, telephone numbers, and personal identification document information, into the Western Union Money Transfer System to pay the fraudulently-induced transfers to the Fraudsters or retransfer the funds to other complicit Western Union Agent locations elsewhere. The corrupt Western Union Agents would take a cut of the ill-gotten proceeds. In all such scenarios, Western Union received its transaction fees.

66. Thirty-nine (39) Western Union Agents have been charged in the United States with defrauding consumers through various schemes including fraudulent sweepstakes, advance fee loans, fake business opportunities (including "secret shopper" or work-at-home scams), emergency or person-in-need scams, and Internet purchase offers. The charges included conspiracy to commit mail fraud, wire fraud and money laundering. Most of the Agents have already pleaded guilty or have been convicted of the charges.

67. Western Union Agents and Sub-agents also assisted or supported Fraudsters by paying out funds in violation of Western Union's policies and procedures.

68. Defendants failed to promptly investigate, suspend, and terminate Agents and Sub-agents that exhibited high levels of consumer fraud, some of which were likely complicit in



frauds, or which ignored such frauds by failing to comply with Western Union's policies and procedures.

69. Defendants permitted Agents and Sub-agents that had processed hundreds of thousands of dollars, or even millions of dollars, in confirmed and potential fraud to continue operating for months or even years, despite highly suspicious activities and indications of complicity.

70. Defendants knew that the Bank Secrecy Act ("BSA") required Western Union to monitor international Agents and take corrective action against Agents violating laws or regulations. Nevertheless, Defendants purposefully failed to implement or execute effective disciplinary policies, and act on its employees' recommendations to discipline, suspend, or terminate international Agent locations. As a result, complicit Western Union Agent locations remained open for years and processed additional fraud transactions to the detriment of Plaintiffs and the other Class members.

71. Nigerian scammers, for example, are at the center of many international frauds. Western Union's Agent Locations in Nigeria pay out large numbers of fraud-induced money transfers and engage in other suspicious activities, and approximately 86.7% of those transfers came from the United States. In February 2012, the U.S. Secret Service warned Western Union that: its services were "widely used by Nigerian scammers and other criminal elements overseas"; "a person in America can easily be robbed by someone in a foreign country and there is almost no possibility to recover that fraud loss"; its "services are widely used for online scams in the US"; and Western Union "is a complete and almost total safe haven for the criminal element to freely launder illegal proceeds without detection." Despite repeated reviews and

investigations of Western Union's Agent locations in Nigeria, as of October 2015, Defendants rarely, if ever, terminated them for consumer fraud.

72. Similarly, from July 2009 to as recently as August 2015, an Agent location in Malaysia made payouts relating to at least 252 fraud complaints totaling \$389,061. Although the Agent appeared on fraud reports and was reviewed for fraud many times between 2010 and 2014, the Agent was not terminated. In fact, in 2014, Western Union executives approved the reactivation of that Agent despite being informed that confirmed and potential fraud, as well as suspicious activity, amounted to approximately 54% of the agent's pay volume.

73. Likewise, an Agent location in Greece made payouts relating to at least 106 fraud complaints totaling \$193,696 from July 2013 to October 2014. From 2012 to 2014, the agent paid out \$5.4 million in money transfers, of which approximately \$3.7 million were for \$1,000 or more. That Agent operated for over two years despite appearing on internal fraud or Agent complicity index reports multiple times and being reviewed for fraud at least three times with findings of suspicious activities.

74. And from September 2013 to August 2015, an Agent in Thailand paid out money transfers associated with at least 1,197 complaints totaling \$425,409, of which 336 complaints totaling \$117,290 were paid out in April 2015 alone. That Agent was allowed to continue operating, despite a review in 2013 finding that 63% of the Agent's transactions in two months amounted to confirmed fraud and questionable activity, and a review in 2015 associated with three of its agent ID numbers finding that 25% of its activity in one month, amounting to over \$1.2 million, was connected to fraud.

75. Defendants purposefully ignored useful suggestions and recommendations from employees and representatives of law enforcement agencies. These types of measures include,

but are not limited to: (a) bolstering ID requirements for sending or receiving money transfers, such as by imposing more robust ID requirements; (b) requiring the collection of additional biographical information; implementing more controls for noncompliant transactions or potentially fraud-induced money transfers, including, but not limited to, transactions with data integrity issues and to high-risk countries; (c) improving the company's handling of, and ability to receive, complaints about fraud worldwide; and (d) improving its interdiction system to be more effective in blocking money transfers associated with consumer fraud, including, but not limited to, by permanently blocking payouts to the recipients of fraud-induced money transfers.

76. Western Union employees recommended specific actions, policies, and procedures to take action against potentially complicit Western Union Agent locations, but Defendants rejected those recommendations. For example:

a. Global Guidelines: As early as 2004, an employee in Western Union's Corporate Security Department prepared a set of "draft" Global Guidelines for disciplining and suspending Western Union Agent Locations worldwide that processed a materially elevated number of reported fraud transactions. In these guidelines, the employee proposed mandatory review of any Agent location that paid ten CFRs within 60 days. The Corporate Security employee further proposed automatically suspending any Agent location that paid five or more transactions reported as fraud within 60 days of a review. In other words, the Corporate Security employee proposed automatically suspending any Agent location that paid fifteen (15) CFRs within 120 days. Western Union rejected the proposed Global Guidelines and did not implement them.

b. 60-Day Fraud Report: As early as 2005, Western Union's Corporate Security Department used CFRs to generate a regular 60-Day Fraud Report, which identified

Agent locations that processed five or more CFRs within 60 days. Corporate Security distributed the report to a broad group of Western Union employees, including Western Union senior employees, and cautioned that Agent locations that did not “drastically reduce” payments of transactions identified in CFRs within 60 days would be suspended. Even though Corporate Security threatened to suspend Agent locations, thousands of complicit Western Union Agent locations—particularly international locations—appeared on the 60-Day Fraud Report multiple times with increasing CFR payments without Western Union taking disciplinary action against them.

c. Agent Fraud Complicity Programs: In January 2008, two Western Union departments separately proposed methods to discipline potentially complicit Western Union Agent locations. One proposal specifically warned against the influence of sales employees on any Agent location disciplinary process because sales employees’ “compensation is often based on agent performance—so they ... see no reason good enough to hold their agent responsible” for fraud transactions. A Western Union senior vice president said she was “coordinating the many functions in the company that look at ... data which might indicate an agent, a location, or an agent employee is engaged in illegal activities.” She was “focused on ... analysis of the consumer fraud complaints ... from a risk-based approach, separating out agent locations ... that are complicit and need to be suspended.... [And] the need to enhance processes” at Western Union. Western Union’s then-Chief Compliance Officer wrote, “I am in favor of this proposal with two caveats: The necessary resource commitment - the more we look [for Agent involvement in fraud schemes] the more we find... and I’d like this communicated in the appropriate way so that everyone understands their roles and responsibilities.” Western Union failed to implement either of the proposed disciplinary programs.

77. Had Western Union implemented the proposed Global Guidelines or the other proposed policies listed above, it could have prevented significant fraud losses to victims. Specifically, the proposed Global Guidelines would have resulted in potential suspensions and terminations against more than 2,000 Agent locations worldwide. Had Western Union implemented the proposed Global Guidelines, it would have stopped these same Agent Locations from processing more than \$174 million in reported fraud losses.

78. Further, as stated in the January 2018 New York Consent Order, Western Union management intervened, on numerous occasions, to obtain more lenient treatment for certain New York Agents, which were some of the Company's highest fee generators.

79. For example, a Western Union compliance employee explained by e-mail to a business executive that compliance staff would give "plenty of notice before they conduct reviews with agents who have 2 or more probations," apparently maximizing the chance for such Agents to avoid more serious discipline, and a corresponding suspension or cessation of fee revenue.

80. As another example, rather than suspend a high fee-generating New York Agent for multiple legal and policy violations, Company management actually paid the Agent a \$250,000 bonus to renew the contract with Western Union.

81. In fact, Western Union refused to terminate Agents and Sub-agents engaged in fraudulent conduct despite agreeing to do so.

82. In November 2005, Western Union entered into an agreement with the Attorneys General of 47 states and the District of Columbia (the "NAAG Agreement") to resolve the states' investigations into fraud transactions at Western Union. As part of the NAAG Agreement, Western Union promised to terminate any Agent—domestic or international—that was

“complicit in fraud-induced transfers or knowingly ignore[d] such fraud, or, if certain employees of the agent or subagent are the [sic] complicit ignoring parties, insist upon termination of such employees as a condition to continued agent or subagent status.” Western Union also agreed to suspend or terminate Agents that failed to take reasonable steps to reduce fraud transactions.

83. After entering into the NAAG Agreement, however, Western Union neither implemented nor maintained effective policies or procedures to suspend or terminate international Agents that processed fraud payments.

84. Further, in some cases, Defendants installed Agents or Sub-agents that Western Union had previously terminated, that were previously suspended or terminated by MoneyGram for fraud, or that were concurrently operating as MoneyGram agents (in violation of Western Union’s Agent agreements).

85. For example, in 2006, a Western Union Agent in College Park, Georgia was suspended due to consumer fraud, but began operating again in 2007 from the same address, but with a different business name and agent ID number, until the Agent was suspended for fraud again. The Agent then became a MoneyGram agent and continued to generate fraud-induced money transfers for approximately one year before being terminated by MoneyGram. After that, the Agent returned to Western Union in 2009, and began operating for a third time with the same name and at the same location. A review in 2012 revealed that approximately 80% of its payouts were attributable to fraud, and it was later terminated. In 2015, the Agent began operating again as a Western Union Agent from the same address, using a similar name, but with a new agent ID number, and once again, it began generating fraud complaints.

86. As another example, after suspending an Agent location in the Philippines due to high levels of fraud, Western Union discovered that the owner of the location had been a high-

volume sender to Nigeria who Western Union had blocked just two months before the location began operating. During the three-month period before the Agent location was suspended, it generated at least 173 fraud complaints totaling \$316,400, and paid out over \$1.2 million in suspected fraud.

87. Moreover, despite receiving information from consumers, their family members, or law enforcement representatives about fraud-induced money transfers, Defendants did not record information about all of those money transfers in Western Union's complaint database.

88. Western Union uses the information in its complaint database to administer its anti-fraud program, so it is imperative that the database is accurate and complete. For example, Western Union uses this information to: (a) monitor and identify Agents and Sub-agents that may be complicit in frauds; (b) create automated rules regarding particular corridors (*e.g.*, limiting the number and amount of money transfers to receivers); and (c) interdict individuals who are the victims or the perpetrators of frauds. Therefore, Defendants' failure to keep accurate and complete records of fraud-induced money transfers has impeded Western Union's efforts to detect and prevent such fraud from occurring.

89. Although Western Union employees have brought the underreporting of fraud-induced money transfers in the company's complaint database to the attention of those responsible for maintaining the database, Defendants have failed to take adequate corrective action, if any, to address the problem.

90. Further, although FinCEN, the primary administrator of the BSA, requires money services businesses like Western Union to file Suspicious Activity Reports ("SARs") relating to fraud, Defendants have, in many cases, failed to file SARs on, and identify as the subject of

SARs, particular Agent locations in foreign countries that have processed high levels of fraud-induced money transfers sent by U.S. consumers and exhibited other suspicious activities

91. In addition to its anti-fraud program, Western Union is required by the BSA to have an effective AML program to guard against money laundering, including, but not limited to, guarding against the flow of illicit funds, such as funds derived from fraud. As part of its AML program, Western Union has developed “Know Your Agent” guidelines and policies, and policies and procedures for monitoring transaction, customer, and agent activity for risks, including suspicious activity and agent complicity. Western Union’s AML program relies heavily upon its agents to have their own AML programs. In many cases, Defendants have failed to implement effective AML policies and procedures pertaining to consumer fraud, thereby making Western Union’s Money Transfer System more vulnerable to such fraud.

92. Further, up until in or around December 2011, Defendants did not provide any toll-free number that consumers in countries other than the United States and Canada could use to report fraud and to try to stop the payout of a fraud-induced money transfer. For example, Western Union did not provide fraud hotlines for consumers in Germany, Mexico, Spain, and the United Kingdom until December 2011, for consumers in Australia, Japan, and Malaysia until February 2012, and for consumers in Austria, Belgium, Luxembourg, and Switzerland until August 2012.

93. Further, Defendants made it difficult for employees to take meaningful action to detect and prevent consumer fraud, including by failing to provide employees with sufficient information or resources, including complete records of consumer fraud complaints, as well as information about law enforcement contacts, investigations, and actions. For many years,



departments within Western Union responsible for handling consumer fraud issues failed to routinely share consumer fraud information with other groups or departments.

94. Further, for many years, the department at Western Union primarily responsible for conducting background checks was not provided with sufficient information to conduct thorough background checks of every prospective and existing Agent and Sub-agent, such as information from law enforcement, information about investigations of Agent locations, and access to consumer complaints.

95. Further, although Western Union has ostensibly relied on its Agents to comply with Western Union's anti-fraud and AML programs, and to oversee the activity of their own Sub-agents and locations, Defendants have not provided Agents with the information necessary to conduct effective fraud reviews and to detect and prevent consumer fraud, including the potential complicity of particular Agent locations. For example, Western Union typically has not shared with the Agents themselves complaints it has received about fraud-induced money transfers processed by the Agent locations. Therefore, despite being tasked with overseeing the conduct of their own Sub-agents and Agent locations, Western Union's Agents, in many cases, are unaware of the nature, details, history, and volume of complaints involving the Agent locations.

96. Defendants have also not effectively trained, monitored, and reviewed Agents and Sub-agents to detect and prevent consumer fraud and to prevent potential complicity at Agent locations.

97. Agents and Sub-agents responsible for processing fraud-induced money transfers were ignorant of Western Union's anti-fraud and policies and procedures, including detecting and preventing fraud, properly recording customers' biographical information and IDs, and

addressing suspicious activities. Western Union also did not have an adequate and effective system in place to ensure that Agents are knowledgeable in these areas. As a result, in many instances, Western Union's high-fraud Agent locations have violated the Company's policies and procedures by failing to collect proper IDs or biographical information from recipients of money transfers, accepting improper forms of IDs, or recording obviously incorrect or fictitious ID information into Western Union's system.

98. Despite Western Union's 2005 Agreement with the States, which required Western Union to "commence a program of person-to-person or telephone training at agent locations known to have a materially elevated level of outgoing or incoming fraud-induced transfers sent from the United States to anywhere except Mexico," Western Union failed to implement such a program at many such Agents locations. For example, with respect to many of its foreign Agent locations that have exhibited high fraud levels, Western Union's practice was only to train the master Agents and not to conduct person-to-person or telephone training at the Agent locations that exhibited high levels of fraud.

99. Western Union failed to conduct adequate and routine onsite compliance reviews of its Agent locations worldwide. Western Union often relied on its master Agents to conduct reviews, but failed to ensure that those master Agents were conducting adequate and effective oversight of their subagents and Locations. In other cases, Western Union's employees were unable to conduct independent, on-site reviews of certain Locations because they were in areas considered too dangerous to visit. Western Union also failed to conduct adequate and routine onsite reviews of many of its independent Agents.

100. For many years, consumer fraud was not even routinely addressed in Western Union's compliance reviews of Agents. Even after it was added to the list of topics for these

reviews, consumer fraud for many years was addressed only in a cursory manner. In addition, in many instances, Western Union employees who conducted compliance reviews were not provided with information about fraud complaints involving the Agents being reviewed, so the employees could not adequately address issues related to the complaints in their reviews.

101. Further, in many instances, Western Union employees responsible for monitoring the activities of Agent locations were not provided with sufficient information or resources to adequately monitor Western Union's Agents, Sub-agents, and Agent locations. For example, in some instances, Western Union assigned more than one agent ID number to a single Agent or Sub-agent without providing Western Union employees with the means to easily locate all of the Agent's or Sub-agent's ID numbers in Western Union's system. Western Union similarly failed to provide its employees with the means to easily identify Agents or Sub-agents with common ownership. In addition, in some cases, Western Union's employees were unable to identify problematic Agents because Agents have not used unique IDs when processing money transfers. Western Union's employees also sometimes have not had complete and historical information about particular Agents and Sub-agents, including information about all fraud complaints, prior reviews, investigations, and internal reports related to fraud, as well as transactional activity. Therefore, Western Union employees responsible for monitoring Agent activity may not have been aware of all relevant information.

102. Western Union and its Agents also failed to provide adequate and effective warnings to consumers about the fraud occurring through its Money Transfer System. Although Western Union provides some warnings on the first page of "send" forms located at some of its Agent locations, in many cases, these warnings are unclear and inconspicuous.

103. In addition, Western Union's Agent locations failed to provide routine verbal warnings to consumers before they initiated money transfers, even in instances where consumers' money transfers displayed obvious signs of fraud, such as high-dollar money transfers by elderly consumers to countries known for fraud. Therefore, consumers often have been unaware of the risks associated with sending money through Western Union's Money Transfer System.

104. Even after January 2011, when Western Union claimed in a written report to have implemented "a comprehensive anti-fraud program" to protect consumers, Defendants still had not adopted an adequate and effective anti-fraud program.

105. Although, as a result of the FTC's investigation, Western Union has improved aspects of its anti-fraud program since 2012, Defendants still have not promptly terminated Agents around the world that appear to be complicit in paying out the fraud-induced money transfers, including, for example, numerous Agents in Spain that operated between January 2011 and December 2012, and were arrested by the Spanish police in 2014 for their role in laundering large sums of money received from the fraud victims. As of October 2015, Defendants rarely, if ever, terminated Agent locations for fraud in certain high-risk countries, including, but not limited to, Mexico, Nigeria, Ghana, the Dominican Republic, China, and Haiti, despite high levels of fraud and indications of complicity at Agent locations.

106. Discovery will reveal whether Defendants' involvement in a scheme to defraud through the Western Union Money Transfer System is still ongoing.

**D. *The Amount of Actual Fraud is Significantly Higher than What Was Reported in, and Subject to, the DPA.***

107. On information and belief, the actual consumer losses due to fraud perpetrated through Western Union far exceed the approximately \$500 million loss figure reported in the DPA.

108. The losses reported in the DPA were based on information in Western Union's CFR database. The CFR database, however, includes information representative of only a small percentage of the actual fraud perpetrated through Western Union's Money Transfer System.

109. The majority of fraud victims do not complain directly to Western Union. Western Union's own internal reports recognize that only a small percentage of consumers complain about fraud and that the volume of fraud-induced money transfers is much higher than that reported to the Company. For example, in several reports, Western Union has recognized that the actual amount of fraud-induced money transfers associated with agent locations was, in some cases, more than five times higher than the reported complaint figures.

110. Further, Western Union's CFR database is incomplete because Western Union has failed to log into its CFR database all of the complaints and reports about fraud it has received, as well as all of the fraud-induced money transfers related to those complaints.

111. Thus, the CFR database significantly understates the number of actual fraud-induced money transfers and losses. Since January 1, 2004, it is likely that Western Union's Money Transfer System has been used to send billions of dollars in fraud-induced payments to con artists worldwide, at the expense of Plaintiffs and the other Class members.

**E. *Equitable Tolling***

112. The findings in the DPA and FTC Complaint were based on facts uniquely within Western Union's knowledge.

113. Innocent consumers, including Plaintiffs and the other Class members, had no knowledge of the facts asserted above before the government released its findings in January 2017. Nor did consumers, including Plaintiffs and the other Class members, have access to Western Union's internal documents that would have revealed Defendants' complicity and involvement in an overarching scheme to defraud, including Western Union's own analyses demonstrating and confirming their complicity with Fraudsters, misrepresentations to the public, and violations of BSA and FinCEN requirements.

114. Further, Western Union continually and falsely asserted that it was an ethical and responsible business that tried to prevent fraud. For example, Western Union affirmatively misleads consumers by representing on its website: "Western Union is dedicated to fighting fraud and helping consumers protect themselves from falling victim to fraud,"<sup>4</sup> and omitting that it actually does the opposite.

115. And, as another example, in its Corporate Responsibility Report, Western Union asserted that it "stand[s] up for customers" and made false representations regarding its commitment to preventing fraud.<sup>5</sup> In relevant part, Western Union falsely asserted:

a. "We also strive to create a culture of compliance and promote ethical conduct throughout our global operations."

b. "We seek to adhere to high standards of corporate governance. This begins with a board of directors who are engaged and knowledgeable about our business, and committed to establishing and maintaining high standards of ethics and integrity for our Company."

---

<sup>4</sup> <https://www.westernunion.com/us/en/fraudawareness/fraud-home.html>.

<sup>5</sup> *See, e.g.*, 2014 Corporate Responsibility Report, available at [https://corporate.westernunion.com/documents/WUReportInteractive\\_%20jul2014\\_%20Lowres\\_single.pdf](https://corporate.westernunion.com/documents/WUReportInteractive_%20jul2014_%20Lowres_single.pdf).

c. “We care about the people who use our services; we know they work hard for their money.”

d. “We also work hard to educate the public about various types of consumer fraud and how they can protect themselves.”

e. “Our tradition of consumer protection and empowerment includes fraud prevention measures, competitive services, data security and privacy measures, transparency in marketing, and a commitment to those we serve.”

f. “While people are critical to compliance, system controls provide an additional measure of protection. We continue to expand and improve our system controls. They are used to help monitor Agent compliance with regulatory and internal requirements and minimize the element of human error.”

g. “The GMI [Global Monitoring and Intelligence] team is trained to watch for signs of possible money laundering, fraud or terrorist financing. We monitor consumers, Agents and geographies for indications of undesirable activity and potential system abuse. Our Financial Intelligence Unit is designed to research and investigate potential money laundering complicity by Agents and incidents of money transfer activity that could indicate money laundering. Our approach combines data analysis and risk assessment techniques to identify and, where appropriate, act upon potentially suspicious activity.”

h. “Protecting customers from fraud is one of our priorities. Western Union’s Anti-Fraud Program emphasizes consumer education and awareness, fraud monitoring, fraud controls, and collaboration with law enforcement as well as consumer advocacy organizations.”

i. “Consumer protection and empowerment is an issue of considerable importance to Western Union, and something we work to address on many levels.”

j. “Western Union regularly reviews its Anti-Fraud Program and adjusts its controls to respond to evolving and emerging trends – much like law enforcement must do when confronting sophisticated and organized criminals. While technology has innumerable benefits, it also has given con artists widely expanded opportunities to scam people via email, websites and phone. Anyone can be a victim of a scam. Unfortunately, there are relationship scams aimed at people seeking companionship, lottery scams aimed at people’s desire to win money and prizes, Internet purchase scams that take advantage of people who shop online, and job scams for those who are looking for work. Whether it is working to help prevent these scams or raise awareness of new ones, we take a multi-pronged approach: building consumer awareness, training our Agents, investing in technological solutions and collaborating with law enforcement.”

k. “Agents are trained to help identify potential fraud victims. If an Agent suspects that the transaction is fraudulent, the Agent is trained to refuse the transaction or report it to Western Union for further investigation. Our Agents are on the front lines of customer service. Therefore we support and empower them with tools and techniques to prevent fraud by providing a variety of Agent training resources and materials through channels that include fraud kits, newsletters, fraud alerts and an online Agent Resource Center. . . . We also analyze Agent activity, along with fraud complaints received from consumers, and determine whether Agents need additional training or oversight, or if they should be suspended or even terminated. These reviews have led to program enhancements, including additional controls for transactions and additional training and support where needed.”



l. “We employ proprietary systems, policies and procedures to help us seek to identify and stop transactions that may be fraudulent. In addition to consumer and Agent education, Western Union has implemented a number of controls designed to stop fraudulent transactions before they are paid. For instance, our Courtesy Callback Program is a critical component of our consumer protection efforts in some countries. As part of this program, Western Union may try to contact senders whose transactions meet certain criteria to interview them in an attempt to determine if they are victims of fraud. If consumer fraud is detected, the principal and fees for the money transfer are refunded to the sender.”

m. “Operating Ethically: Western Union moves money for better in more than 200 countries and territories around the world and is subject to myriad laws and regulations. We take those requirements seriously, and strive to meet the highest standards of compliance and ethical conduct throughout our global operations. We are known and trusted by millions, and we endeavor to earn – and keep – that trust every day.”

n. “Conducting Our Business with Integrity: Western Union has been providing reliable services to consumers for more than 160 years. Operating with integrity is of the utmost importance to us, and we believe this commitment is one key to our long-term business success. For us, this involves maintaining respect for employees and providing them access to the tools and training they need to help them better serve our customers. . . . Like any financial institution, laws addressing consumer protection, data privacy, safety and soundness apply in jurisdictions where we do business. We take these requirements seriously, as do our Agents. They are a reflection of – and also supported by – our core values.”

o. “Our Core Values – Integrity - We do business each day with an absolute commitment to ethics, honesty and credibility.”

p. “Western Union maintains a commitment to a culture of ethics and integrity. The Western Union Code of Conduct provides guidance to employees in fulfilling their responsibility for compliance with Company policy and the laws and regulations that apply to our business around the world. Western Union sponsors multiple programs and resources for employee compliance education as well as established channels to ask questions or raise concerns. The annual performance evaluations of employees include a rating on the Culture of Compliance performance objective.”

116. *None* of these statements were true. Rather, Western Union made those statements—and also omitted and failed to disclose material facts to Plaintiffs and the other Class members—for the sole reason of misleading and deflecting any investigation into Western Union’s potential culpability for the above-described fraudulent conduct.

117. No amount of due diligence by innocent consumers, including Plaintiffs and the other Class members, could have uncovered Defendants’ involvement and complicity in the systematic fraud.

118. Indeed, as demonstrated by Plaintiffs’ own conduct, as alleged herein, Western Union’s customer service told them that their losses had nothing to do with Western Union and that Western Union couldn’t do anything to help them.

## **V. CLASS ACTION ALLEGATIONS**

119. Plaintiffs bring this action pursuant to Rules 23(a), 23(b)(2), and 23(b)(3) of the Federal Rules of Civil Procedure individually and on behalf of all others similarly situated.

120. Plaintiffs seek to represent a Class defined as:

All consumers in the United States who were defrauded through Western Union’s Money Transfer System from January 1, 2004 to the present.

121. Excluded from the Class are Defendants and any of their members, affiliates, parents, subsidiaries, officers, directors, employees, successors, or assigns; the judicial officers and their immediate family members; and Court staff assigned to this case. Plaintiffs reserve the right to modify or amend the Class definition, as appropriate, during the course of this litigation.

122. This action may be brought and maintained pursuant to Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, and satisfies all predicate requirements thereof.

123. **Numerosity: Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. While Plaintiffs are informed and believe that there are hundreds of thousands of Class members, the precise number of Class members is presently unknown to Plaintiffs, but will be determined through discovery. Class members' names and addresses are available from Defendants' records, and Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. Mail, electronic mail, Internet postings, and/or published notice.

124. **Commonality and Predominance: Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** This action involves common questions of law and fact, which predominate over any questions affecting individual Class members, including, without limitation:

- a. Whether Defendants engaged in the conduct alleged herein;
- b. Whether Defendants sent interstate or international wires as part of a scheme to defraud;
- c. Whether Defendants conspired to send interstate or international wires as part of a scheme to defraud;

- d. Whether Defendants participated in the conduct of an enterprise's affairs by sending interstate or international wires as part of a scheme to defraud;
- e. Whether Plaintiffs and the other Class members were damaged as a result of Defendants' scheme to defraud;
- f. Whether Defendants concealed their participation in their scheme to defraud until January 19, 2017; and
- g. The amount and nature of relief to be awarded to Plaintiffs and the other Class members.

125. **Typicality: Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of the other Class members' claims because Plaintiffs and the other Class members were subjected to the same allegedly unlawful conduct and damaged in the same way by Defendants.

126. **Adequacy of Representation: Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are adequate class representatives because their interests do not conflict with the interests of the other Class members who they seek to represent, Plaintiffs have retained counsel competent and experienced in complex class action litigation and RICO, and Plaintiffs intend to vigorously prosecute this action. Plaintiffs and their counsel will fairly and adequately protect the Class's interests.

127. **Declaratory and Injunctive Relief: Federal Rule of Civil Procedure 23(b)(2).** Defendants have acted or refused to act on grounds generally applicable to the Class members, thereby making appropriate final injunctive relief and declaratory relief, as described below, with respect to the Class members as a whole.

128. **Superiority: Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy,

and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for the Class members to individually seek redress for Defendants' wrongful conduct. Even if the Class members could afford litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

## **VI. CLAIMS ALLEGED**

### **FIRST CLAIM FOR RELIEF**

#### **Violations of 18 U.S.C. § 1962(c) and (d) (Against All Defendants)**

130. Plaintiffs repeat, reallege, and incorporate by reference the allegations set forth in Paragraphs 1-129 of this Complaint as though fully set forth herein.

131. Plaintiffs bring this claim individually and on behalf of the other Class members, as defined in Paragraph 120 of this Complaint. This claim, which alleges violations of Section 1962(c) and (d) of RICO, 18 U.S.C. § 1962(c) & (d), is asserted against Defendant Hikmet Ersek and the Doe Defendants who are the directors, officers, managers, and employees of TWUC and/or WUFSI who were complicit in the intentional scheme and who, as alleged in Paragraph 27, will be specifically identified during the course of reasonable fact discovery. This claim is also asserted against Defendant TWUC and Defendant WUFSI.

132. At all relevant times, each of the Plaintiffs, each of the other Class members, Defendant Hikmet Ersek, each of the Doe Defendants, Defendant TWUC, and Defendant

WUFSI was an individual or an entity capable of holding a legal or beneficial interest in property, which means that each of them is a “person” within the meaning of Sections 1961(3) and 1962(c) of RICO, 18 U.S.C. § 1961(3) & 1962(c).

133. **The TWUC-WUFSI Corporate Enterprise:** At all relevant times, there existed an “enterprise,” within the meaning of Sections 1961(4) and 1962(c) of RICO, 18 U.S.C. § 1961(4) & 1962(c), an association-in-fact comprised of two independent entities, TWUC and WUFSI (the “TWUC-WUFSI Corporate Enterprise”). The TWUC-WUFSI Corporate Enterprise’s lawful purpose was the acceptance and delivery of wire transfers in interstate and foreign commerce. The TWUC-WUFSI Corporate Enterprise’s unlawful purpose was to engage in and carry out an intentional scheme to defraud users of its lawful service of vast sums of money. Its continuity was coterminous with the period of time necessary to defraud Plaintiffs and the other Class members.

134. The TWUC-WUFSI Corporate Enterprise was engaged in, and its activities affected, interstate and foreign commerce. At all relevant times, as the relevant directors, officers, managers and/or key employees, the Doe Defendants were employed by and/or associated with the TWUC-WUFSI Corporate Enterprise. In violation of Section 1962(c) of RICO, 18 U.S.C. § 1962(c), Defendant Hikmet Ersek and the Doe Defendants conducted or participated, directly or indirectly, in the conduct of the TWUC-WUFSI Corporate Enterprise’s affairs through a pattern of racketeering activity by engaging in multiple, repeated, and continuous violations of the federal wire fraud statute, 18 U.S.C. § 1343. As set forth herein, Defendant Hikmet Ersek and the Doe Defendants transmitted, or caused to be transmitted, by wires, communications of Plaintiffs and the other Class members, in interstate or foreign commerce to designated persons for ostensibly legitimate purposes, but with the actual, unlawful

purpose of engaging in an intentional scheme to defraud Plaintiffs and the other Class members of vast sums of money.

135. In violation of Section 1962(d) of RICO, 18 U.S.C. § 1962(d), Defendant Hikmet Ersek and the Doe Defendants conspired to violate Section 1962(c) of RICO.

136. **The Western Union Money Transfer Enterprise:** In the alternative, at all relevant times, there existed an “enterprise,” within the meaning of Sections 1961(4) and 1962(c) of RICO, 18 U.S.C. § 1961(4) & 1962(c), to wit, an association-in-fact comprised of TWUC, WUFISI, and the Independent Agents. The Western Union Money Transfer Enterprise’s lawful purpose was the acceptance and delivery of wire transfers in interstate and foreign commerce. The Western Union Money Transfer Enterprise’ unlawful purpose was to engage in and carry out an intentional scheme to defraud users of its lawful service of vast sums of money. Its continuity was coterminous with the period of time necessary to defraud Plaintiffs and the other Class members.

137. The Western Union Money Transfer Enterprise was engaged in, and its activities affected, interstate and foreign commerce. At all relevant times, Defendant TWUC and Defendant WUFISI were employed by and/or associated with the Western Union Money Transfer Enterprise. In violation of Section 1962(c) of RICO, 18 U.S.C. § 1962(c), Defendant TWUC and Defendant WUFISI conducted or participated, directly or indirectly, in the conduct of the affairs of the Western Union Money Transfer Enterprise through a pattern of racketeering activity by engaging in multiple, repeated, and continuous violations of the federal wire fraud statute, 18 U.S.C. § 1343. As set forth herein, Defendant TWUC and Defendant WUFISI transmitted, or caused to be transmitted, by wires, communications of Plaintiffs and the other Class members, in interstate or foreign commerce to designated persons for ostensibly legitimate

purposes, but with the actual, unlawful purpose of engaging in an intentional scheme to defraud Plaintiffs and the other Class members of vast sums of money.

138. In violation of Section 1962(d) of RICO, 18 U.S.C. § 1962(d), Defendant TWUC and Defendant WUFSI conspired to violate Section 1962(c) of RICO.

139. At all relevant times, the Western Union Corporate Enterprise and the Western Union Money Transfer Enterprise were engaged in, and their activities affected, both interstate and foreign commerce.

140. By reason of the above-referenced violations of Section 1962(c) and (d) of RICO, 18 U.S.C. § 1962(c) & (d), Plaintiffs and the other Class members have been injured in their business or property within 18 U.S. § 1964(c) of RICO, and Plaintiffs and the other Class members are entitled to assert this claim and recover threefold the damages they sustained and the cost of the suit, including reasonable attorneys' fees, and other appropriate relief.

**SECOND CLAIM FOR RELIEF**  
**Violations of 18 U.S.C. § 1962(b) and (d)**  
**(Against Defendant TWUC and Defendant WUFSI)**

141. Plaintiffs repeat, reallege, and incorporate by reference the allegations set forth in Paragraphs 1-129 of this Complaint as though fully set forth herein.

142. Plaintiffs bring this claim individually and on behalf of the other members of the Class, as defined in Paragraph 120 of this Complaint. This claim, which alleges violations of Section 1962(b) and (d) of RICO, 18 U.S.C. § 1962(b) & (d), is asserted against Defendant TWUC and Defendant WUFSI.

143. At all relevant times, each of the Plaintiffs, each of the other Class members, Defendant TWUC, and Defendant WUFSI was an individual or an entity capable of holding a



legal or beneficial interest in property, which means that each of them is a “person” within the meaning of Sections 1961(3) and 1962(c) of RICO, 18 U.S.C. § 1961(3) & 1962(c).

144. At all relevant times, each of the Plaintiffs and each of the other Class members who was an “individual” or a “legal entity” was an “enterprise” within the meaning of Sections 1961(4) and 1962(b) of RICO, 18 U.S.C. § 1961(4) & 1962(b).

145. Each of the Plaintiffs and each of the other Class members was engaged in interstate or foreign commerce when he, she, or it wired money through Western Union’s Money Transfer System.

146. As set forth herein, Defendant TWUC and Defendant WUFSI transmitted, or caused to be transmitted, by wires, communications of Plaintiffs and the other Class members, in interstate or foreign commerce to designated persons for ostensibly legitimate purposes, but with the actual, unlawful purpose of facilitating an intentional scheme to defraud Plaintiffs and the other Class members of vast sums of money.

147. As set forth herein, Defendant TWUC and Defendant WUFSI engaged in a pattern of racketeering activity by engaging in multiple, repeated, and continuous violations of the federal wire fraud statute.

148. In violation of Section 1962(b) of RICO, 18 U.S.C. § 1962(b), and through the above-referenced pattern of racketeering activity, Defendant TWUC and Defendant WUFSI acquired an interest (proceeds) of the enterprise—to wit, Plaintiffs and the other Class members— when they caused Plaintiffs and the other Class members to enter into transactions that they otherwise would not have entered into.

149. In violation of Section 1962(d) of RICO, 18 U.S.C. § 1962(d), Defendant TWUC and Defendant WUFSI conspired to violate Section 1962(b) of RICO.

150. By reason of the above-referenced violations of Section 1962(b) and (d) of RICO, 18 U.S.C. § 1962(b) & (d), Plaintiffs and the other Class members have been injured in their business or property within 18 U.S. § 1964(c) of RICO, and Plaintiffs and the other Class members are entitled to assert this claim and recover threefold the damages they sustained and the cost of the suit, including reasonable attorneys' fees, and other appropriate relief.

**THIRD CLAIM FOR RELIEF**  
**Violations of Colo. Rev. Stat. Ann. § 18-17-104(3) and (4)**  
**(Against All Defendants)**

151. Plaintiffs repeat, reallege, and incorporate by reference the allegations set forth in Paragraphs 1-129 of this Complaint as though fully set forth herein.

152. Plaintiffs bring this claim individually and on behalf of the other members of the Class, as defined in Paragraph 120 of this Complaint. This claim, which alleges violations of Section 18-17-104(3) and (4) of the Colorado Organized Crime Control Statute ("COCCA"), Colo. Rev. Stat. Ann. § 18-17-104(3) & (4), is asserted against Defendant Hikmet Ersek and the Doe Defendants who are the relevant directors, officers, managers, and employees of TWUC and/or WUFSI who were knowingly complicit in the intentional scheme to defraud and who, as alleged in Paragraph 27, will be specifically identified during the course of reasonable fact discovery. This claim is also asserted against Defendant TWUC and Defendant WUFSI.

153. At all relevant times, each of the Plaintiffs, each of the other Class members, Defendant Hikmet Ersek, each of the Doe Defendants, Defendant TWUC, and Defendant WUFSI was an individual or an entity capable of holding a legal or beneficial interest in property, which means that each of them is a "person" within the meaning of Sections 18-17-103(4) and 18-17-104(3) of COCCA.

154. **The TWUC-WUFSI Corporate Enterprise:** At all relevant times, there existed an “enterprise,” within the meaning of Sections 18-17-103(2) and 18-17-104(3) of COCCA—to wit, an association-in-fact comprised of two independent entities, TWUC and WUFSI (the “TWUC-WUFSI Corporate Enterprise”). The TWUC-WUFSI Corporate Enterprise’s lawful purpose was the acceptance and delivery of wire transfers in interstate and foreign commerce. The TWUC-WUFSI Corporate Enterprise’s unlawful purpose was to engage in and carry out an intentional scheme to defraud users of its lawful service of vast sums of money. Its continuity was coterminous with the period of time necessary to defraud Plaintiffs and the other Class members. At all relevant times, as the relevant directors, officers, managers and/or key employees, Defendant Hikmet Ersek and the Doe Defendants were employed by and/or associated with the TWUC-WUFSI Corporate Enterprise. In violation of Section 18-17-104(3) of COCCA, Defendant Hikmet Ersek and the Doe Defendants knowingly conducted or participated, directly or indirectly, in the TWUC-WUFSI Corporate Enterprise through a pattern of racketeering activity related to the enterprise by engaging in multiple and repeated violations of the federal wire fraud statute, 18 U.S.C. § 1343. As set forth herein, Defendant Hikmet Ersek and the Doe Defendants transmitted, or caused to be transmitted, by wires, communications of Plaintiffs and the other Class members, in interstate or foreign commerce to designated persons for ostensibly legitimate purposes, but with the actual, unlawful purpose of facilitating an intentional scheme to defraud Plaintiffs and the other Class members of vast sums of money.

155. In violation of Section 18-17-104(4) of COCCA, Defendant Hikmet Ersek and the Doe Defendants conspired to violate Section 18-17-104(3) of COCCA.

156. **The Western Union Money Transfer Enterprise:** In the alternative, at all relevant times, there existed an “enterprise,” within the meaning of Sections 18-17-103(2) and

18-17-104(3) of COCCA—to wit, an association-in-fact comprised of TWUC, WUFSI, and the Independent Agents. The Western Union Money Transfer Enterprise’s lawful purpose was the acceptance and delivery of wire transfers in interstate and foreign commerce. The Western Union Money Transfer Enterprise’s unlawful purpose was to engage in and carry out an intentional scheme to defraud users of its lawful service of vast sums of money. Its continuity was coterminous with the period of time necessary to defraud Plaintiffs and the other Class members. At all relevant times, Defendant TWUC and Defendant WUFSI were employed by and/or associated with the Western Union Money Transfer Enterprise. In violation of Section 18-17-104(3) of COCCA, Defendant TWUC and Defendant WUFSI conducted or participated, directly or indirectly, in such Western Union Money Transfer Enterprise through a pattern of racketeering activity related to the enterprise by knowingly engaging in multiple and repeated violations of the federal wire fraud statute, 18 U.S.C. § 1343. As set forth herein, Defendant TWUC and Defendant WUFSI transmitted, or caused to be transmitted, by wires, communications of Plaintiffs and the other Class members in interstate or foreign commerce to designated persons for ostensibly legitimate purposes, but with the actual, unlawful purpose of engaging an intentional scheme to defraud Plaintiffs and the other Class members of vast sums of money.

157. In violation of Section 18-17-104(4) of COCCA, Defendant TWUC and Defendant WUFSI conspired to violate Section 18-17-104(3) of COCCA.

158. By reason of the above-referenced violations of Section 18-17-104(3) and (4) of COCCA, Plaintiffs and the other Class members have been injured within Section 18-17-106(7) of COCCA, and Plaintiffs and the other Class members are entitled to assert this claim and

recover threefold the damages they sustained and the cost of the suit, including reasonable attorneys' fees, and other appropriate relief.

**FOURTH CLAIM FOR RELIEF**  
**Violations of Colo. Rev. Stat. Ann. § 18-17-104(2) and (4)**  
**(Against Defendant TWUC and Defendant WUFSI)**

159. Plaintiffs repeat, reallege, and incorporate by reference the allegations set forth in Paragraphs 1-129 of this Complaint as though fully set forth herein.

160. Plaintiffs bring this claim individually and on behalf of the other members of the Class, as defined in Paragraph 121 of this Complaint. This claim, which alleges violations of Section 18-17-104(2) and (4) of COCCA, is asserted against Defendant TWUC and Defendant WUFSI.

161. At all relevant times, each of the Plaintiffs, each of the other Class members, Defendant TWUC, and Defendant WUFSI was an individual or an entity capable of holding a legal or beneficial interest in property, which means that each of them is a "person" within the meaning of Sections 18-17-103(4) and 18-17-104(2) of COCCA.

162. At all relevant times, each of the Plaintiffs and each of the other Class members who was an "individual" or a "legal entity" was an "enterprise" within the meaning of Sections 18-17-103(2) and 18-17-104(2) of COCCA.

163. As set forth herein, Defendant TWUC and Defendant WUFSI transmitted, or caused to be transmitted, by wires, communications of Plaintiffs and Class members, in interstate or foreign commerce to designated persons for ostensibly legitimate purposes, but with the actual, unlawful purpose of facilitating an intentional scheme to defraud Plaintiffs and the other Class members of vast sums of money.

164. As set forth herein, Defendant TWUC and Defendant WUFSI knowingly engaged in a pattern of racketeering activity related to the enterprise by engaging in multiple and repeated violations of the federal wire fraud statute.

165. In violation of Section 18-17-104(2) of COCCA, and through the above-referenced pattern of racketeering activity, Defendant TWUC and Defendant WUFSI acquired an interest (proceeds) of the enterprise—to wit, Plaintiffs and the other Class members—when they caused Plaintiffs and the other Class members to enter into transactions that they otherwise would not have entered into.

166. In violation of Section 18-17-104(4) of COCCA, Defendant TWUC and Defendant WUFSI conspired to violate Section 18-17-104(2) of COCCA.

167. By reason of the above-referenced violations of Sections 18-17-104(2) and (4) of COCCA, Plaintiffs and the other Class members have been injured in their business or property within Section 18-17-106(7) of COCCA, and Plaintiffs and the other Class members are entitled to assert this claim and recover threefold the damages they sustained and the cost of the suit, including reasonable attorneys' fees, and other appropriate relief.

**FIFTH CLAIM FOR RELIEF**  
**Violations of Colo. Rev. Stat. § 18-4-405**  
**(Against Defendant TWUC and Defendant WUFSI)**

168. Plaintiffs repeat, reallege, and incorporate by reference the allegations set forth in Paragraphs 1-129, above, as though fully set forth herein.

169. Plaintiffs bring this claim individually and on behalf of the other members of the Class, as defined in Paragraph 120 of this Complaint. This claim for civil theft, pursuant to Colo. Rev. Stat. § 18-4-405, is asserted against Defendant TWUC and Defendant WUFSI.

170. Defendant TWUC and Defendant WUFSI knowingly obtained and exercised control over monies belonging to Plaintiffs and the other Class members. Defendant TWUC and Defendant WUFSI knowingly obtained and exercised control over monies provided by Plaintiffs and the other Class members to be transferred using Western Union's Money Transfer System. Defendant TWUC and Defendant WUFSI knowingly obtained and exercised control over fees paid by Plaintiffs and the other Class members in connection with the transfer of money through Western Union's Money Transfer System.

171. Defendant TWUC and Defendant WUFSI's control over monies belonging to Plaintiffs and the other Class members was unauthorized, and achieved through deception, because Defendant TWUC and Defendant WUFSI collected the monies under the false pretense that they would be facilitating a legitimate transfer through Western Union's Money Transfer System. Plaintiffs and the other Class members did not authorize Defendant TWUC and Defendant WFUSI to transfer monies to third-party Fraudsters or collect fees for the transfer of money to third-party Fraudsters.

172. By transferring monies to third-party Fraudsters, and keeping fees collected in connection with the transfer of money to third-party Fraudsters, Defendant TWUC and Defendant WUFSI, knowingly and intentionally, permanently deprived Plaintiffs and the other Class members of their monies, and of the use and benefit of their monies.

173. As a direct and proximate result of Defendant TWUC and Defendant WUFSI's misconduct, Plaintiffs and the other Class members have incurred damages in an amount to be determined at trial. Pursuant to Colo. Rev. Stat. § 18-4-405, Plaintiffs and the other Class members are entitled to three times the amount of actual damages sustained, as well as the cost of the suit and reasonable attorneys' fees.

**SIXTH CLAIM FOR RELIEF**  
**Negligence**  
**(Against Defendant TWUC and Defendant WUFSI)**

174. Plaintiffs repeat, reallege, and incorporate by reference the allegations set forth in Paragraphs 1-129, above, as though fully set forth herein.

175. Plaintiffs bring this claim individually and on behalf of the other members of the Class, as defined in Paragraph 120 of this Complaint. This claim, which alleges common law negligence, is asserted against Defendant TWUC and Defendant WUFSI.

176. Defendant TWUC and Defendant WUFSI were aware that the Western Union Money Transfer System was used for rampant fraud and deceit.

177. Defendant TWUC and Defendant WUFSI each had a duty of care to consumers, including Plaintiffs and the other Class members, transmitting money through the Western Union Money Transfer System.

178. Defendant TWUC and Defendant WUFSI could foresee that there was an unreasonably high probability that its customers, including Plaintiffs and the other Class members, would be defrauded by third-party Fraudsters if they did not implement reasonable anti-fraud measures, including complying with FinCEN and BSA requirements.

179. Defendant TWUC and Defendant WUFSI failed to implement reasonable anti-fraud measures, including complying with FinCEN and BSA requirements.

180. Due to Defendant TWUC's and Defendant WUFSI's failure to implement reasonable anti-fraud measures, including complying with FinCEN and BSA requirements, Plaintiffs and the other Class members suffered financial harm.



181. As a direct and proximate result of Defendant TWUC's and Defendant WUFISI's negligence, Plaintiffs and the other Class members have incurred damages in an amount to be determined at trial.

**SEVENTH CLAIM FOR RELIEF**  
**Unjust Enrichment**  
**(Against Defendant TWUC and Defendant WUFISI)**

182. Plaintiffs repeat, reallege, and incorporate by reference the allegations set forth in Paragraphs 1-129, above, as though fully set forth herein.

183. Plaintiffs bring this claim individually and on behalf of the other members of the Class, as defined in Paragraph 120 of this Complaint. This unjust enrichment claim is asserted against Defendant TWUC and Defendant WUFISI.

184. Plaintiffs and the other Class members conferred a benefit on Defendant TWUC and Defendant WUFISI when they paid fees to Defendant TWUC and Defendant WUFISI for the transfer of money to third-party Fraudsters through Western Union's Money Transfer System.

185. Defendant TWUC and Defendant WUFISI have retained the benefit conferred by Plaintiffs and the other Class members.

186. Plaintiffs and the other Class members received nothing in return for the benefit conferred on Defendant TWUC and Defendant WUFISI.

187. Defendant TWUC and Defendant WUFISI were complicit in, and/or acted recklessly and negligently with respect to, the systemic fraud being perpetrated through the Western Union Money Transfer System.

188. Plaintiffs and the other Class members were unaware that Defendant TWUC and Defendant WUFISI was complicit in, and/or acted recklessly and negligently with respect to, the systemic fraud being perpetrated through the Western Union Money Transfer System.

189. Defendant TWUC and Defendant WUFSI knowingly accepted the unjust benefits of its wrongful conduct, and it is inequitable and unconscionable for Defendant TWUC and Defendant WUFSI to retain these benefits. As a result of Defendant TWUC's and Defendant WUFSI's misconduct, the amount of its unjust enrichment should be disgorged and returned to Plaintiffs and the other Class members in an amount to be proven at trial.

**EIGHTH CLAIM FOR RELIEF**  
**Conversion**  
**(Against Defendant TWUC and Defendant WUFSI)**

190. Plaintiffs repeat, reallege, and incorporate by reference the allegations set forth in Paragraphs 1-129, above, as though fully set forth herein.

191. Plaintiffs bring this claim individually and on behalf of the other members of the Class, as defined in Paragraph 120 of this Complaint. This conversion claim is asserted against Defendant TWUC and Defendant WUFSI.

192. Defendant TWUC and Defendant WUFSI exercised dominion and control over monies belonging to Plaintiffs and the other Class members. Defendant TWUC and Defendant WUFSI exercised dominion and control over monies provided by Plaintiffs and the other Class members to be transferred using Western Union's Money Transfer System. Defendant TWUC and Defendant WUFSI also exercised dominion and control over fees paid by Plaintiffs and the other Class members in connection with the transfer of money through Western Union's Money Transfer System.

193. Defendant TWUC and Defendant WUFSI's dominion and control over monies belonging to Plaintiffs and the other Class members was unauthorized because Defendant TWUC and Defendant WUFSI collected the monies under the false pretense that they would be facilitating a legitimate transfer through Western Union's Money Transfer System. Plaintiffs

and the other Class members did not authorize Defendant TWUC and Defendant WFUSI to transfer monies to third-party Fraudsters or collect fees for the transfer of money to third-party Fraudsters.

194. By transferring monies to third-party Fraudsters, and keeping fees collected in connection with the transfer of money to third-party Fraudsters, Defendant TWUC and Defendant WUFSI wrongfully deprived Plaintiffs and the other Class members of their property.

195. Defendant TWUC and Defendant WUFSI have completed conversion of the monies collected from Plaintiffs and the other Class members.

196. As a direct and proximate result of Defendant TWUC and Defendant WUFSI's misconduct, Plaintiffs and the other Class members have incurred damages in an amount to be determined at trial.

#### **VII. JURY DEMAND**

Plaintiffs demand a trial by jury.

#### **VIII. REQUEST FOR RELIEF**

WHEREFORE, Plaintiffs, individually and on behalf of the other Class members, respectfully request that the Court enter judgment in their favor and against Defendants, jointly and severally, on each claim for relief as follows:

1. Declaring that this action is a proper class action, certifying the Class, as requested herein, designating Plaintiffs as Class Representatives, and appointing Plaintiffs' attorneys as Class Counsel;

2. Enjoining Defendants from continuing to engage in the illegal practices described herein;

3. Ordering Defendants to pay actual, statutory, treble, and punitive damages to Plaintiffs and the other Class members, as allowable by law;
4. Ordering Defendants to pay restitution to Plaintiffs and the other Class members, as allowable by law;
5. Ordering Defendants to provide an accounting to Plaintiffs and the other Class members, and to disgorge all proceeds illegally obtained by the Defendants and for which they were unjustly enriched;
6. Ordering Defendants to pay both pre- and post-judgment interest on any amounts awarded;
7. Ordering Defendants to pay attorneys' fees and costs of suit; and
8. Ordering such other and further relief as may be just and proper.

Dated: April 26, 2018

Respectfully submitted,

*s/ Ty Gee*

\_\_\_\_\_  
Ty Gee

**HADDON, MORGAN AND FOREMAN P.C.**

150 East 10th Avenue

Denver, Colorado 80203

Telephone: 303-831-7364

tgee@hmflaw.com

Adam J. Levitt (*pro hac vice* motion to be filed)

Daniel R. Ferri (*pro hac vice* motion to be filed)

**DICELLO LEVITT & CASEY LLC**

Ten North Dearborn Street, Eleventh Floor

Chicago, Illinois 60602

Telephone: 312-214-7900

alevitt@dlcfirm.com

dferri@dlcfirm.com

Kevin P. Roddy (*pro hac vice* motion to be filed)  
**WILENTZ, GOLDMAN & SPITZER, P.A.**  
90 Woodbridge Center Drive, Suite 900  
Woodbridge, New Jersey 07095  
Telephone: 732-636-8000  
kroddy@wilentz.com

Kenneth S. Canfield  
**DOFFERMYRE SHIELDS CANFIELD &  
KNOWLES, LLC**  
1355 Peachtree Street, Suite 1900  
Atlanta, Georgia 30309  
Telephone: 404-881-8900  
kcanfield@dsckd.com

G. Robert Blakey (*pro hac vice* motion to be filed)  
**WILLIAM J. & DOROTHY T. O'NEILL  
PROFESSOR OF LAW EMERITUS  
NOTRE DAME LAW SCHOOL\***  
7002 East San Miguel Avenue  
Paradise Valley, Arizona 85253  
Telephone: 574-514-8220  
blakey.1@nd.edu  
\*For purposes of identification only

***Counsel for Plaintiffs and the Proposed Class***

**IN THE UNITED STATES DISTRICT COURT  
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA**

<b>UNITED STATES OF AMERICA,</b>	:	
	:	
<b>Plaintiff</b>	:	
	:	<b>CRIMINAL No.</b>
	:	
<b>v.</b>	:	
	:	<b>(Judge            )</b>
	:	
<b>THE WESTERN UNION COMPANY,</b>	:	
	:	
<b>Defendant</b>	:	

**DEFERRED PROSECUTION AGREEMENT**

Defendant THE WESTERN UNION COMPANY (“Western Union” or the “Company”), by its undersigned representatives, pursuant to authority granted by the Company’s Board of Directors, and the United States Department of Justice, Criminal Division, Money Laundering and Asset Recovery Section, the United States Attorney’s Offices for the Middle District of Pennsylvania, the Central District of California, the Eastern District of Pennsylvania, and the Southern District of Florida (collectively, the “Offices”), enter into this Deferred Prosecution Agreement (the “Agreement”), the terms and conditions of which are as follows:

**Criminal Information and Acceptance of Responsibility**

1. The Company acknowledges and agrees that the Offices will file the attached two count criminal Information in the United States District Court for the Middle District of Pennsylvania charging the Company with (1) willfully failing to implement an effective anti-money laundering program, in violation of Title 31, United States Code, Sections 5318(h) and 5322 and regulations issued thereunder; and (2) aiding and abetting wire fraud, in violation of

Title 18, United States Code, Sections 1343 and 2. In so doing, the Company: (a) knowingly waives its right to indictment on these charges, as well as all rights to a speedy trial pursuant to the Sixth Amendment to the United States Constitution, Title 18, United States Code, Section 3161, and Federal Rule of Criminal Procedure 48(b); and (b) knowingly waives for the purposes of this Agreement and for the purposes of any charges by the United States arising out of the conduct described in the attached Statement of Facts any objection with respect to venue and consents to the filing of the Information, as provided under the terms of this Agreement, in the United States District Court for the Middle District of Pennsylvania. The Offices agree to defer prosecution of the Company pursuant to the terms and conditions described below.

2. “Western Union Agent” or “Agents” are generally individuals or entities that own and/or operate businesses that have a contractual relationship with Western Union and, by virtue of that contractual relationship are authorized to offer Western Union’s money transfers to consumers. Western Union Agents may have multiple locations where Western Union services are offered. In the U.S., Western Union directly contracts with both network agents and independent agents. Network agents are retail chains that have one contract with Western Union through which the retailer offers Western Union services at multiple locations. Independent agents are small independent businesses such as convenience stores that contract directly with Western Union to offer Western Union services at their locations. In some countries outside the U.S., Western Union may operate through master agents, which are generally independent businesses that in turn subcontract with generally small independent stores who offer Western Union services at their locations. All Western Union Agent locations have access to the Money Transfer System and must send all Western Union transfers by wire via the Money Transfer

System. “Western Union Agent” or “Agents” include, but are not limited to, network, independent, master, or subagents. The Company admits, accepts, and acknowledges that it is responsible under United States law for the acts of its officers, directors, and employees, as well as for certain conduct of its Agents, such as use of Western Union’s money transfer system, as charged in the Information, and as set forth in the Statement of Facts attached hereto as Attachment A and incorporated by reference into this Agreement, and that the allegations described in the Information and the facts described in Attachment A are true and accurate. Should the Offices pursue the prosecution that is deferred by this Agreement, the Company stipulates to the admissibility of the Statement of Facts in any proceeding, including any trial, guilty plea, or sentencing proceeding, and will not contradict anything in the Statement of Facts at any such proceeding.

#### **Term of the Agreement**

3. This Agreement is effective for a period beginning on the date on which the Information is filed and ending three (3) years from the later of the date on which the Information is filed or the date on which the Court enters the Agreement. However, the Company agrees that in the event that the Offices determine, in their sole discretion, subject to the notice and opportunity to respond provisions in Paragraph 16, that the Company has knowingly violated any provision of this Agreement, an extension or extensions of the Term of the Agreement may be imposed by the Offices, in their sole discretion, for up to a total additional time period of one year, without prejudice to the Offices’ right to proceed as provided in Paragraphs 15 through 18 below. Any extension of the Agreement extends all terms of this Agreement. Conversely, in the event the Offices find, in their sole discretion, that the provisions



of this Agreement have been satisfied, the Term of the Agreement may be terminated early. If the Court rejects the Agreement, all the provisions of the Agreement, including all attachments to and representations in this Agreement, shall be deemed null and void, and the Term shall be deemed to have not begun.

#### **Relevant Considerations**

4. The Offices enter into this Agreement based on the individual facts and circumstances presented by this case and the Company. Among the factors considered were the following:

a. the seriousness of the conduct described in the Statement of Facts including the high-dollar amount of fraud-related and structured funds that the Company transmitted, and misconduct that spanned multiple jurisdictions and was known throughout the Company;

b. the Company's willingness to acknowledge and accept responsibility for its conduct;

c. the Company's significant compliance enhancements since at least 2012 designed to improve its anti-money laundering and anti-fraud compliance programs, which demonstrate the Company's commitment to maintaining and enhancing the effectiveness of its compliance program;

d. the Company's commitment to continue to enhance its anti-money laundering and anti-fraud compliance programs, including implementing and complying with the Enhanced Compliance Undertaking in Attachment C;

e. the Company's cooperation with law enforcement;

f. the Company's agreement to provide the Offices with access to and reports by the independent auditor retained pursuant the Federal Trade Commission ("FTC") stipulated Order;

g. the Company's agreement to cooperate with the Offices as described in Paragraph 5 below; and

h. the Company's willingness to settle any and all civil and criminal claims currently held by the Offices for any act within the scope of the Statement of Facts.

**Future Cooperation and Disclosure Requirements**

5. The Company shall cooperate fully with the Offices in any and all matters relating to the conduct described in this Agreement and the Statement of Facts and other conduct under investigation by the Offices or any other component of the Department of Justice at any time during the Term of the Agreement, subject to applicable law and regulations, until the later of the date upon which all investigations and prosecutions arising out of such conduct are concluded, or the end of the Term of the Agreement. At the request of the Offices, the Company shall also cooperate fully with other federal law enforcement and regulatory authorities and agencies, in any investigation of the Company, its subsidiaries or affiliates, or any of its present or former officers, directors, employees, Agents, Agent employees, consultants, or any other party, in any and all matters relating to the conduct described in this Agreement and the Statement of Facts and other conduct under investigation by the Offices or any component of the Department of Justice at any time during the Term of the Agreement. The Company agrees that its cooperation shall include, but not be limited to, the following:

a. The Company shall truthfully disclose all factual information relating to the conduct described in this Agreement and the Statement of Facts and other conduct under investigation by the Offices or any other component of the Department of Justice at any time during the Term of the Agreement in the possession of the Company or its subsidiaries not protected by a valid claim of attorney-client privilege or work product doctrine, with respect to its activities, those of its subsidiaries and affiliates, and those of its present or former directors, officers, employees, Agents, Agent employees, and consultants, including any evidence or allegations and internal or external investigations, or information learned from the FTC Auditor, about which the Company has any knowledge or about which the Offices may inquire. This obligation of truthful disclosure includes, but is not limited to, the obligation of the Company to provide to the Offices, upon request, any document, record or other tangible evidence about which the Offices may inquire of the Company, subject to applicable law and regulations;

b. Upon request of the Offices, the Company shall designate knowledgeable employees, agents or attorneys to provide the Offices the information and materials described in Paragraph 5(a) above on behalf of the Company. It is further understood that the Company must at all times provide complete, truthful, and accurate information;

c. The Company shall use its best efforts to make available for interviews or testimony, as requested by the Offices, present or former officers, directors, employees, Agents, Agent employees, and consultants of the Company, concerning the matters set forth in Paragraph 5(a). This obligation includes, but is not limited to, sworn testimony before a federal grand jury or in federal trials, as well as interviews with federal law enforcement and regulatory authorities, concerning the matters set forth in Paragraph 5(a). Cooperation under this Paragraph shall

include identification of witnesses who, to the knowledge of the Company, may have material information regarding the matters under investigation;

d. With respect to any information, testimony, documents, records or other tangible evidence provided to the Offices pursuant to this Agreement, the Company consents to any and all disclosures, subject to applicable law and regulations, to other governmental authorities, including United States authorities and those of a foreign government, of such materials as the Offices, in their sole discretion, shall deem appropriate; and

e. If the Company cannot cooperate with the obligations in Paragraph 5 due to applicable law, regulations, or a valid claim of privilege, the Company will provide a log listing a general description of the information withheld, the applicable law, regulation, or privilege that prevents disclosure of the information requested, and a detailed statement explaining why the applicable law, regulation, or privilege prevents disclosure.

6. In addition to the obligations in Paragraph 5 above, during the Term of the Agreement, should the Company learn of credible evidence or allegations of criminal violations of U.S. federal law by the Company or its subsidiaries or affiliates, or any of its present or former officers, directors, employees, Agents, Agent employees, or consultants, the Company shall promptly report such evidence or allegations to the Offices.

#### **Forfeiture Amount**

7. As a result of Western Union's conduct, including the conduct set forth in the Statement of Facts, the parties agree that each of the Offices could institute a civil and/or criminal forfeiture action against certain funds held by Western Union and that such funds would be forfeitable pursuant to Title 18, United States Code, Sections 981 and 982 and Title 28,

United States Code, Section 2461(c). Western Union hereby acknowledges that at least \$586 million in consumer fraud proceeds are traceable to transactions in violation of Title 18, United States Code, Sections 1343 and 2, as described in the Statement of Facts. Western Union hereby agrees to forfeit to the United States the sum of \$586 million (the “Forfeiture Amount”). The Offices are collecting the Forfeiture Amount in this manner to make the funds available to compensate victims of the fraud scheme described in the Statement of Facts, pursuant to 18 U.S.C. § 981(e)(6), under the Petition for Remission and/or Mitigation procedures of the United States Department of Justice or any other manner within the United States Attorney General’s discretion. The Company hereby agrees that, in the event the funds used to pay the Forfeiture Amount are not directly traceable to the transactions, the monies used to pay the Forfeiture Amount shall be considered substitute *res* for the purpose of forfeiture to the United States pursuant to Title 18, United States Code, Sections 981, 982 or Title 28, United States Code, Section 2461(c), and the Company releases any and all claims it may have to such funds. The Company shall pay \$146.5 million of the Forfeiture Amount plus any associated transfer fees within five (5) business days of the date on which this Agreement is signed, pursuant to payment instructions provided by the Offices in their sole discretion. The Company shall pay the remaining sum of \$439.5 million plus any associated transfer fees within ninety (90) business days of the date this Agreement is signed, pursuant to payment instructions provided by the Offices in their sole discretion. The Company agrees to sign any additional documents necessary to complete forfeiture of the funds.

8. The Forfeiture Amount paid is final and shall not be refunded should the Government later determine that the Company has breached this Agreement and commences a

prosecution against the Company. In the event of a breach of this Agreement and subsequent prosecution, the Offices are not limited to the Forfeiture Amount. The Offices agree that in the event of a subsequent breach and prosecution, it will recommend to the Court that the amounts paid pursuant to this Agreement be offset against whatever forfeiture the Court shall impose as part of its judgment. The Company understands that such a recommendation will not be binding on the Court.

**Conditional Release from Liability**

9. Subject to Paragraphs 15 through 18 below, the Offices agree, except as provided herein, that they will not bring any criminal or civil case against the Company or any of its wholly owned or controlled subsidiaries relating to any of the conduct described in the Statement of Facts, attached hereto as Attachment A, the criminal Information filed pursuant to this Agreement, or information that the Company disclosed to the Offices prior to the date of the Agreement. The Offices, however, may use any information related to the conduct described in the attached Statement of Facts against the Company in a: (a) prosecution for perjury or obstruction of justice; (b) prosecution for making a false statement; or (c) prosecution or other proceeding relating to a violation of any provision of Title 26 of the United States Code.

a. This Agreement does not provide any protection against prosecution for any future conduct by the Company.

b. In addition, this Agreement does not provide any protection against prosecution of any present or former officer, director, employee, shareholder, Agent, Agent employee, consultant, contractor, or subcontractor of the Company for any violations committed by them.

### **Corporate Compliance Program**

10. The Company represents that it has implemented and will continue to implement a compliance program reasonably designed to prevent and detect violations of the Bank Secrecy Act (“BSA”), money laundering statutes, and other specified unlawful activity throughout its operations, including those of its affiliates, Agents, and joint ventures, and those of its contractors and subcontractors whose responsibilities include providing money transfer services as required by law or regulation, Attachment C, or the FTC order.

11. In order to address any deficiencies in its anti-money laundering and anti-fraud programs, the Company represents that it has undertaken, and will continue to undertake in the future, in a manner consistent with all of its obligations under this Agreement, review and enhancement of its anti-money laundering and anti-fraud program, policies, procedures, and controls. If necessary and appropriate, the Company will adopt new or modify existing programs, reasonably designed policies, procedures, and controls in order to ensure that the company maintains: (a) effective anti-money laundering and anti-fraud programs; and (b) Agent oversight policies, including reasonably designed procedures and controls designed to detect, deter, and discipline violations of the BSA, money laundering, fraud and gambling statutes by Agents and their owners, employees, officers, directors, consultants, contractors, or subcontractors. The reasonably designed anti-money laundering and anti-fraud programs, policies, procedures and controls will include, but not be limited to, the minimum elements set forth in Attachment C, which is incorporated by reference into this Agreement.

12. The Company shall comply with the FTC Auditor Agreement and provide the FTC auditor reports to the Offices at the same time as provided to the FTC.

**Deferred Prosecution**

13. In consideration of: (a) the past and future cooperation of the Company described in Paragraph 5 above; (b) the Company's agreement to forfeiture of \$586 million; and (c) the Company's implementation and maintenance of compliance enhancements as described in Paragraphs 10 through 12 above and Attachment C, the Offices agree that any prosecution of the Company for the conduct set forth in the Statement of Facts be and hereby is deferred for the Term of this Agreement.

14. The Offices further agree that if the Company fully complies with all of its obligations under this Agreement, the Offices will not continue the criminal prosecution against the Company described in Paragraph 1 and, at the conclusion of the Term, this Agreement shall expire. Within three (3) months of the Agreement's expiration, the Offices shall seek dismissal with prejudice of the criminal Information filed against the Company described in Paragraph 1 above, and agrees not to file charges in the future against the Company based on the conduct described in this Agreement and Attachment A.

**Breach of the Agreement**

15. If, during the Term of the Agreement, the Company (a) commits any felony under U.S. federal law; (b) provides in connection with this Agreement deliberately false, incomplete, or misleading information; (c) fails to cooperate as set forth in Paragraphs 5 and 6 of this Agreement; (d) fails to put into effect or operation, implement, and maintain a compliance program as set forth in Paragraphs 10 through 12 of this Agreement and Attachment C; or (e) otherwise fails to specifically perform or to fulfill completely each of the Company's obligations under the Agreement, regardless of whether the Offices become aware of such a breach after the



Term of the Agreement is complete, the Company shall thereafter be subject to prosecution for any federal criminal violation of which the Offices have knowledge, including, but not limited to, the charges in the Information described in Paragraph 1 and charges that arise from the conduct set forth in the Statement of Facts, which may be pursued by the Offices in the U.S. District Courts for the Middle District of Pennsylvania, the Central District of California, the Eastern District of Pennsylvania, or the Southern District of Florida, or any other appropriate venue. Determination of whether the Company has breached the Agreement and whether to pursue prosecution of the Company shall be in the Offices' sole discretion, subject to the notice and opportunity to respond provisions in Paragraph 16. Any such prosecution may be premised on information provided by the Company or its personnel, Agents, or Agent employees. Any such prosecution relating to the conduct described in the Statement of Facts or relating to conduct known to the Offices prior to the date on which this Agreement was signed that is not time-barred by the applicable statute of limitations on the date of the signing of this Agreement may be commenced against the Company notwithstanding the expiration of the statute of limitations between the signing of this Agreement and the expiration of the Term of the Agreement plus one year. Thus, by signing this Agreement, the Company agrees that the statute of limitations with respect to any such prosecution that is not time-barred on the date of the signing of this Agreement shall be tolled for the Term of the Agreement plus six months. In addition, the Company agrees that the statute of limitations as to any violation of federal law that occurs during the Term of the Agreement will be tolled from the date upon which the violation occurs for the duration of the Term of the Agreement plus six months, and that this period shall

be excluded from any calculation of time for purposes of the application of the statute of limitations.

16. In the event that the Offices determine that the Company has breached this Agreement, the Offices agree to provide the Company with written notice of such breach prior to instituting any prosecution resulting from such breach. Within thirty (30) days of receipt of such notice, the Company shall have the opportunity to respond to the Offices in writing to explain the nature and circumstances of such breach, as well as the actions the Company has taken to address and remediate the situation, which explanation the Offices shall consider in determining whether to institute a prosecution.

17. In the event that the Offices determine that the Company has breached this Agreement: (a) all statements made by or on behalf of the Company to the Offices or to the Court, including the attached Statement of Facts, and any testimony given by the Company before a grand jury, a court, or any tribunal, or at any legislative hearings, whether prior or subsequent to this Agreement, and any leads derived from such statements or testimony, shall be admissible in evidence in any and all criminal proceedings brought by the Offices against the Company; and (b) the Company shall not assert any claim under the United States Constitution, Rule 11(f) of the Federal Rules of Criminal Procedure, Rule 410 of the Federal Rules of Evidence, or any other federal rule that any such statements or testimony made by or on behalf of the Company prior or subsequent to this Agreement, or any leads derived therefrom, should be suppressed or are otherwise inadmissible. The decision whether conduct or statements of any current director, officer, or employee, or any person acting on behalf of, or at the direction of, the

Company will be imputed to the Company for the purpose of determining whether the Company has violated any provision of this Agreement shall be in the sole discretion of the Offices.

18. The Company acknowledges that the Offices have made no representations, assurances, or promises concerning what sentence may be imposed by the Court if the Company breaches this Agreement and this matter proceeds to judgment. The Company further acknowledges that any such sentence is solely within the discretion of the Court and that nothing in this Agreement binds or restricts the Court in the exercise of such discretion.

19. Thirty (30) days after the expiration of the period of deferred prosecution specified in this Agreement, the Company, by the Chief Executive Officer and the Chief Compliance Officer of the Company, after conducting a reasonable inquiry within the Company, will certify to the Offices that, in good faith reliance on information provided to the Chief Executive Officer and Chief Compliance Officer by third parties within the Company, and based on their best information and belief, the Company has met its disclosure obligations pursuant to Paragraph 6 of this Agreement. Such certification will be deemed a material statement and representation by the Company to the executive branch of the United States for purposes of Title 18, United States Code Section 1001, and it will be deemed to have been made in the judicial district in which this Agreement is filed.

**Sale, Merger, or Other Change in Corporate Form of Company**

20. Except as may otherwise be agreed by the parties hereto in connection with a particular transaction, the Company agrees that in the event that, during the Term of the Agreement, it undertakes any change in corporate form, including if it sells, merges, or transfers a substantial portion of its business operations as they exist as of the date of this Agreement,

whether such sale is structured as a sale, asset sale, merger, transfer, or other change in corporate form, it shall include in any contract for sale, merger, transfer, or other change in corporate form a provision binding the purchaser, or any successor in interest thereto, to the obligations described in this Agreement. The Company shall provide the Offices at least thirty (30) days' notice prior to undertaking any such sale, merger, transfer, or other change in corporate form, including dissolution, in order to give the Offices an opportunity to determine if such change in corporate form would impact the terms or obligations of the Agreement.

**Public Statements by Company**

21. The Company expressly agrees that it shall not, through present or future attorneys, officers, directors, employees, agents or any other person authorized to speak for the Company make any public statement, in litigation or otherwise, contradicting the acceptance of responsibility by the Company set forth above or the facts described in the Statement of Facts. Any such contradictory statement shall, subject to cure rights of the Company described below, constitute a breach of this Agreement and the Company thereafter shall be subject to prosecution as set forth in Paragraphs 15 through 18 of this Agreement. The decision whether any public statement by any such person contradicting a fact contained in the Statement of Facts will be imputed to the Company for the purpose of determining whether it has breached this Agreement shall be at the sole discretion of the Offices, subject to the notice and opportunity to respond provisions in Paragraph 16. If the Offices determine that a public statement by any such person contradicts in whole or in part information contained in the Statement of Facts, the Offices shall so notify the Company, and the Company may avoid a breach of this Agreement by publicly repudiating such statement(s) within five (5) business days after notification. The Company

shall be permitted to raise defenses and to assert affirmative claims in other proceedings relating to the matters set forth in the Statement of Facts provided that such defenses and claims do not contradict, in whole or in part, a statement contained in the Statement of Facts. This Paragraph does not apply to any statement made by any present or former officer, director, employee, or agent of the Company in the course of any criminal, regulatory, or civil case initiated against such individual, unless such individual is speaking on behalf of the Company.

22. The Company agrees that if it or any of its direct or indirect subsidiaries or affiliates issues a press release or holds any press conference in connection with this Agreement, the Company shall first consult the Offices to determine (a) whether the text of the release or proposed statements at the press conference are true and accurate with respect to matters between the Offices and the Company; and (b) whether the Offices have any objection to the release.

23. The Offices agree, if requested to do so, to bring to the attention of law enforcement and regulatory authorities the facts and circumstances relating to the nature of the conduct underlying this Agreement, including the nature and quality of the Company's cooperation and remediation. By agreeing to provide this information to other authorities, the Offices are not agreeing to advocate on behalf of the Company, but rather are agreeing to provide facts to be evaluated independently by such authorities.

#### **Limitations on Binding Effect of Agreement**

24. This Agreement is binding on the Company and the Offices but specifically does not bind any other component of the Department of Justice, other federal agencies, or any state, local or foreign law enforcement or regulatory agencies, or any other authorities, although the

Offices will, as described in Paragraph 23, discuss the Company's compliance and cooperation with such agencies and authorities if requested to do so by the Company.

**Notice**

25. Any notice to the Offices under this Agreement shall be given by personal delivery, overnight delivery by a recognized delivery service, or registered or certified mail, addressed to Chief, Money Laundering and Asset Recovery Section, Criminal Division, United States Department of Justice, 1400 New York Avenue, Washington, D.C. 20005; the United States Attorney, United States Attorney's Office, Middle District of Pennsylvania, Harrisburg Federal Building and Courthouse, 228 Walnut Street, Suite 220, P.O. Box 11754, Harrisburg, PA 17108-1754; the United States Attorney, United States Attorney's Office, Central District of California, 411 West Fourth Street, Santa Ana, CA 92701; the United States Attorney, United States Attorney's Office, Eastern District of Pennsylvania, 615 Chestnut Street, Suite 1250, Philadelphia, PA 19106; the United States Attorney, United States Attorney's Office, Southern District of Florida, 500 E. Broward Blvd., Ft. Lauderdale, FL, 33394. Any notice to the Company under this Agreement shall be given by personal delivery, overnight delivery by a recognized delivery service, or registered or certified mail, addressed to Western Union, Office of the General Counsel, 12500 East Belford Avenue, Englewood, CO 80112. Notice shall be effective upon actual receipt by the Offices or the Company.

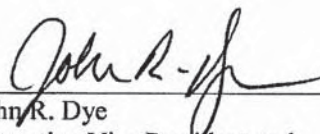
**Complete Agreement**

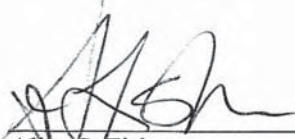
26. This Agreement, including its attachments, sets forth all the terms of the agreement between the Company and the Offices. No amendments, modifications, or additions

to this Agreement shall be valid unless they are in writing and signed by the Offices, the attorneys for the Company, and a duly authorized representative of the Company.

**AGREED:**

**FOR THE WESTERN UNION COMPANY:**

  
\_\_\_\_\_  
John R. Dye  
Executive Vice President and  
General Counsel  
The Western Union Company

  
\_\_\_\_\_  
Alice S. Fisher  
Latham & Watkins LLP  
Counsel to the Company

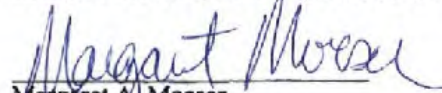


**FOR THE U.S. DEPARTMENT OF JUSTICE:**


BRUCE D. BRANDLER  
United States Attorney  
Middle District of Pennsylvania

  
\_\_\_\_\_  
Kim Douglas Daniel  
Assistant United States Attorney

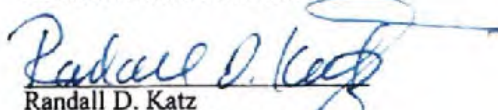
M. KENDALL DAY  
Chief, Money Laundering and  
Asset Recovery Section  
Criminal Division, U.S. Department of Justice

  
\_\_\_\_\_  
Margaret A. Moeser  
Trial Attorney

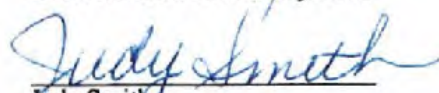
EILEEN M. DECKER  
United States Attorney  
Central District of California

  
\_\_\_\_\_  
Gregory W. Staples  
Assistant United States Attorney

WIFREDO A. FERRER  
United States Attorney  
Southern District of Florida

  
\_\_\_\_\_  
Randall D. Katz  
Assistant United States Attorney

LOUIS D. LAPPEN  
United States Attorney  
Eastern District of Pennsylvania

  
\_\_\_\_\_  
Judy Smith  
Assistant United States Attorney

Date: January 19, 2017

### COMPANY OFFICER'S CERTIFICATE

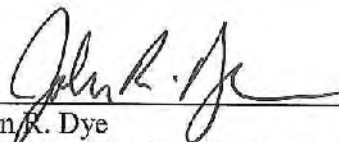
I have read this Agreement and carefully reviewed every part of it with outside counsel for the Western Union Company (the "Company"). I understand the terms of this Agreement and voluntarily agree, on behalf of the Company, to each of its terms. Before signing this Agreement, I consulted outside counsel for the Company. Counsel fully advised me of the rights of the Company, of possible defenses, and of the consequences of entering into this Agreement.

I have carefully reviewed the terms of this Agreement with the Board of Directors of the Company. I have advised and caused outside counsel for the Company to advise the Board of Directors fully of the rights of the Company, of possible defenses, the Sentencing Guidelines' provisions, and of the consequences of entering into the Agreement.

No promises or inducements have been made other than those contained in this Agreement. Furthermore, no one has threatened or forced me, or to my knowledge any person authorizing this Agreement on behalf of the Company, in any way to enter into this Agreement. I am also satisfied with outside counsel's representation in this matter. I certify that I am the Executive Vice President and General Counsel for the Company and that I have been duly authorized by the Company to execute this Agreement on behalf of the Company.

Date: January 16, 2017

THE WESTERN UNION COMPANY

By:   
\_\_\_\_\_  
John A. Dye  
Executive Vice President and General Counsel

### CERTIFICATE OF COUNSEL

I am counsel for the Western Union Company (the "Company") in the matter covered by this Agreement. In connection with such representation, I have examined relevant Company documents and have discussed the terms of this Agreement with the Company Board of Directors. Based on our review of the foregoing materials and discussions, I am of the opinion that the representative of the Company has been duly authorized to enter into this Agreement on behalf of the Company and that this Agreement has been duly and validly authorized, executed, and delivered on behalf of the Company and is a valid and binding obligation of the Company. Further, I have carefully reviewed the terms of this Agreement with the Board of Directors and the Chief Executive Officer of the Company. I have fully advised them of the rights of the Company, of possible defenses, and of the consequences of entering into this Agreement. To my knowledge, the decision of the Company to enter into this Agreement, based on the authorization of the Board of Directors, is an informed and voluntary one.

Date: \_\_\_\_\_

01/18/17

By: \_\_\_\_\_

Alice S. Fisher

Counsel for the Western Union Company

ATTACHMENT A

**STATEMENT OF FACTS**

The following Statement of Facts is incorporated by reference as part of the Deferred Prosecution Agreement (the “Agreement”) between the United States Department of Justice Criminal Division’s Money Laundering and Asset Recovery Section, the United States Attorney’s Offices for the Middle District of Pennsylvania, the Central District of California, the Eastern District of Pennsylvania, and the Southern District of Florida (collectively, the “Department” or the “United States”) and The Western Union Company, (“Western Union” or the “Company”). Certain of the facts herein are based on information obtained from third parties by the United States through their investigation and described to Western Union. The parties stipulate that the allegations in Count One and Two of the Information and the following facts are true and correct, and that were the matter to proceed to trial, the United States would prove them beyond a reasonable doubt, by admissible evidence:

1. Starting in 2004 and ending in December 2012, Western Union violated U.S. laws by (1) willfully failing to implement and maintain an effective anti-money laundering (“AML”) program that was designed to detect, report, and prevent criminals from using Western Union to facilitate their fraud, money laundering, and structuring schemes, and (2) aiding and abetting fraudsters in their unlawful schemes by remaining in business with Agent locations that facilitated the unlawful fraud scheme.
2. Western Union’s conduct included employees (1) repeatedly identifying Western Union Agent locations involved in or facilitating fraud-related transactions but knowingly failing to take effective corrective action; (2) repeatedly identifying Western Union Agents involved in or facilitating unlawful structuring but knowingly failing to take effective corrective action; (3) failing to adequately implement and maintain effective policies and procedures to discipline, suspend, terminate or take effective corrective action against Western Union Agent locations that repeatedly violated the Bank Secrecy Act and other statutes or Western Union anti-money laundering or anti-fraud policies; (4) modifying compliance reviews or results so that Agents with severe compliance failures would not face disciplinary action such as suspension or termination as required by Western Union policies or practices; (5) failing to take effective action to control transactions with characteristics indicative of illegal gaming; or (6) failing to file Suspicious Activity Reports (“SARs”) identifying Western Union Agents as suspicious actors.
3. Fraudsters relied on Western Union’s money transfer system to receive fraud and other criminal proceeds worldwide from victims in the United States. Western Union’s conduct, including its failure to take effective corrective actions in a timely fashion, contributed to the success of the fraudsters’ schemes.
4. This conduct occurred in various Western Union offices and Western Union Agent locations located in the United States and around the world, including, in particular, through wires sent from the Middle District of Pennsylvania in furtherance of the fraud scheme that Western Union aided and abetted.

### Legal Background

5. Congress enacted the Bank Secrecy Act, Title 31, United States Code Section 5311 *et seq.*, and its implementing regulations (collectively the “BSA”) to address an increase in criminal money laundering activity utilizing financial institutions.
6. Western Union is a “financial institution” as defined in the BSA. 31 U.S.C. § 5312(a)(2); 31 C.F.R. § 1010.100. As a financial institution and money services business (“MSB”), Western Union must establish, implement, and maintain an effective AML compliance program that, at a minimum, provides for: (a) internal policies, procedures, and controls to guard against money laundering; (b) an individual or individuals to coordinate and monitor day-to-day compliance with the BSA and AML requirements; (c) an ongoing employee training program; and (d) independent testing of programs. 31 U.S.C. § 5318(h); 31 C.F.R. § 1022.210. Pursuant to 31 U.S.C. § 5322, it is a crime to willfully violate the BSA.
7. In 2004, the U.S. Department of Treasury, Financial Crimes Enforcement Network (“FinCEN”), which is the administrator of the BSA, explained AML program requirements for MSBs with foreign agents like Western Union (the “2004 FinCEN Release”). FinCEN advised that MSBs that use foreign agents to move funds into or out of the United States “must take reasonable steps to guard against the flow of illicit funds, or the flow of funds from legitimate sources to persons seeking to use those funds for illicit purposes” through their foreign agents. Specifically, FinCEN stated that MSB anti-money laundering programs should include procedures for the following:
  - a. conducting reasonable risk-based due diligence on potential and existing foreign agents and counterparties to help ensure that such foreign agents and counterparties are not themselves complicit in illegal activity involving the MSB’s products and services;
  - b. risk-based monitoring and review of transactions from, to, or through the United States that are conducted through foreign agents and counterparties; and
  - c. responding to foreign agents or counterparties that present unreasonable risks of money laundering or the financing of terrorism. Such procedures should provide for the implementation of corrective action on the part of the foreign agent or counterparty or for the termination of the relationship with any foreign agent or counterparty that the MSB determines poses an unacceptable risk of money laundering or terrorist financing, or that has demonstrated systemic, willful, or repeated lapses in compliance with the MSB’s own anti-money laundering procedures or requirements.
8. Under the BSA, financial institutions, including MSBs such as Western Union, must also maintain certain records and file certain reports, including those listed below.
  - a. MSBs must record consumer identification information for the transmittal of funds of more than \$3,000, 12 U.S.C. § 1829b; 31 C.F.R. § 1010.410;

- b. MSBs must file Currency Transaction Reports (“CTRs”), which identify transactions or series of transactions involving currency of more than \$10,000 in one day, 31 U.S.C. § 5313; 31 C.F.R. §§ 1010.311, 1010.313; and
  - c. MSBs must file SARs, which identify transactions of \$2,000 or more that involve or are intended to hide funds derived from illegal activity, are designed to evade BSA requirements, serve no business or lawful purpose, or use the MSB to facilitate criminal activity, 31 U.S.C. § 5318(g); 31 C.F.R. § 1022.320.
9. “Structuring” or breaking transactions into smaller amounts to avoid the BSA’s recordkeeping and reporting requirements is a crime in violation of 31 U.S.C. § 5324. Willfully failing to file SARs is a crime in violation of 31 U.S.C. § 5322.
10. Title 18, United States Code Sections 1343 and 2 make it a crime to use, or aid and abet the use of, interstate wires to carry out a scheme to defraud individuals of money or property by false promises.

### **Western Union Background**

11. Western Union, headquartered in Englewood, Colorado, is a publicly traded company, a financial institution, and one of the largest MSBs in the world. Western Union employs approximately 10,000 individuals worldwide. In 2014, Western Union reported total revenues of \$5.6 billion including more than \$1.56 billion from U.S. operations and more than \$4 billion from international operations. As an MSB, Western Union is currently registered with FinCEN in order to conduct its money transfer business. *See* 31 U.S.C. § 5330; 31 C.F.R. § 1022.380. Most states and many foreign jurisdictions also require financial institutions, such as Western Union, to register or receive a license before offering money transfer services to the public.
12. Western Union’s “Money Transfer System” is an electronic network operated and controlled by Western Union using servers in the United States. Using Western Union’s Money Transfer System, consumers can send money to other individuals in the United States and around the world. Western Union offers its money transfer services to consumers via approximately 550,000 Western Union Agent locations in more than 200 countries and territories. Approximately 90 percent of Western Union Agent locations are located outside the United States. In 2014, more than 150 million individual consumers used Western Union’s Money Transfer System to send or receive more than \$85 billion through Western Union’s Agent locations.
13. Western Union earns revenue by charging consumers a fee based on the money transfer amount and the destination location. Western Union earns additional revenue on international transactions that are sent in one currency and received in a different currency.
14. “Western Union Agents” or “Agents” are generally independent individuals or entities, including banks, post offices, and small independent shops, that own and/or operate businesses that have a contractual relationship with Western Union. By virtue of that contractual relationship, Western Union Agents are authorized to offer Western Union’s

money transfers to consumers. In the U.S., Western Union directly contracts with network and independent Agents. Network Agents are retail chains that have one contract with Western Union through which the retailer offers Western Union services at multiple locations. Independent Agents are small independent businesses such as convenience stores that contract directly with Western Union to offer Western Union services at their locations. Many U.S. Western Union Agents are also MSBs that must comply with the BSA. In some countries outside the U.S., Western Union operates through Master Agents, which are generally independent businesses that in turn subcontract with small independent businesses who offer Western Union services at their locations.

15. Western Union Agents may have multiple locations where Western Union services are offered. Each Western Union Agent location has access to the Money Transfer System and must send all Western Union transfers by wire via the Money Transfer System.
16. Western Union pays Western Union Agents a commission for the money transfers the Agents process. Western Union may also pay the Agents bonuses and other compensation based on transaction volume. Western Union can unilaterally terminate or suspend any Agent or Agent location anywhere in the world for a variety of reasons, including compliance reasons.
17. To send money through Western Union, consumers may go to a Western Union Agent location and give the Agent location information, generally including (1) the sender and payee names, (2) the transfer amount and (3) the state or province and country where the money is to be sent. Sometimes the sender's identification document is required. Consumers give the Western Union Agent location funds to cover the transfer amount and the fee. The Agent enters the transaction into the Money Transfer System and gives the consumer the Money Transfer Control Number ("MTCN"), a ten-digit Western Union reference number for the transaction.
18. To receive a money transfer, the payee typically must appear in person at a Western Union Agent location and provide the Agent location with personal information including the payee's name, address, telephone number, and sometimes the payee's identification document, and the sender's name and location city, state or province, and country, and the expected transfer amount. Paying Western Union Agent locations typically require the payee to provide the MTCN. To complete the transfer to the payee, the paying Agent then transmits this information to the Western Union Money Transfer System via international or interstate wire.
19. The payee can receive the money transfer within minutes after the sender sends the transaction. With certain limited exceptions, Western Union, at its discretion, has the ability to refuse the transaction, or cancel the transaction before the payee receives the transfer from the paying Western Union Agent.
20. "Fraudsters" include, among other individuals involved in the fraud scheme, certain owners, operators and employees of Western Union Agents.

**The Scheme to Defraud Consumers Using the Western Union Money Transfer System**

21. Between 2004 and 2012, Fraudsters engaged in a scheme to defraud consumers through the Western Union Money Transfer System. Certain owners, operators, or employees of Western Union Agent locations were complicit in the scheme (the “Complicit Western Union Agent Locations”). Western Union aided and abetted the Fraudsters’ scheme to defraud by failing to suspend and/or terminate complicit Agents and by allowing them to continue to process fraud induced monetary transactions. The scheme relied on a variety of false promises and other misrepresentations to defraud victims into sending money through Western Union. Fraudsters involved in the scheme contacted victims by phone, U.S. mail, interstate courier, or the Internet, and fraudulently induced them to send money by, among other things:
  - a. falsely promising victims large cash prizes, lottery winnings, fictitious loans, or other payments;
  - b. falsely offering various high-ticket items for sale over the Internet at deeply discounted prices;
  - c. falsely promising employment opportunities as “secret shoppers” who would be paid to evaluate retail stores; or
  - d. falsely posing as the victim’s relative and claiming to be in trouble and in urgent need of money.
22. The Fraudsters told victims that they must send the money in advance to receive the promised outcome. Fraudsters directed the victims to send advance payments to fictitious payees using Western Union’s Money Transfer System.
23. After the victims sent the money through Western Union, the Fraudsters asked them for the Western Union MTCN for the transfer. The Fraudsters took the MTCN to Western Union Agent locations, including Complicit Western Union Agent Locations, who gave the Fraudsters the victims’ money transfers. At no time did the victims receive what the Fraudsters falsely promised them.
24. Certain Complicit Western Union Agent Locations knowingly entered false addresses, telephone numbers, and personal identification document information into the Western Union Money Transfer System in order to pay the fraudulently induced transfers to the Fraudsters or retransfer the funds to other Complicit Western Union Agent Locations elsewhere. Through these actions, the Complicit Western Union Agent Locations concealed the true identities of the Fraudsters, as well as their involvement in the scheme. The Complicit Western Union Agent Locations received money, which was usually subtracted from the victims’ money transfers.
25. Western Union maintained a 1-800 number through which some U.S. victims reported the fraud scheme. Western Union recorded these complaints and others it received in what are known as Consumer Fraud Reports (“CFRs”). The CFRs contain detailed information about the victims, the transactions, and the Western Union Agent locations



that paid the transfers. Western Union maintained a database of all CFRs and used that information to track and investigate Agent locations that paid transfers reported as fraud-induced.

26. Between 2004 and 2012, Western Union's CFRs identified more than \$500 million in reported consumer fraud transactions sent through Western Union Agent locations. Not every victim of the scheme reported the fraud to Western Union. Western Union employees knew that the total amount of fraud was higher than reported fraud as a result of their analyses and internal reports regarding particular Agent locations throughout Western Union's operations.

Western Union Knew Certain of Its Agents Were Complicit in the Scheme to Defraud Using Western Union's Money Transfer System

27. Western Union knew that certain of its Agent locations were complicit in the scheme to defraud using Western Union's Money Transfer System because some of those locations were prosecuted for their criminal activity. For example, between 2001 and 2012, twenty-eight Western Union Agent owners, operators, or employees were charged in the Middle District of Pennsylvania for their participation in fraud or money laundering using Western Union's Money Transfer System.
28. Western Union repeatedly identified Agent locations—particularly overseas Agent locations—that processed high levels of fraud transfers from U.S. victims, including certain Agent locations Western Union suspected were complicit in the fraud scheme, but it took insufficient action to stop these Complicit Agent Locations from facilitating consumer fraud. LJ, a 74 year old resident of the Middle District of Pennsylvania reported that she was the victim of a fraud scheme in October 2012. She attempted to report the fraud to Western Union and a Western Union employee told her that she was “wasting [her] time” reporting the fraud because “there are thousands of these complaints laying on the desk and nothing gets done.” Western Union identified Complicit Western Union Agent Locations through various means, including CFRs, transaction monitoring, and regular reports generated by Western Union analysts reviewing transactions that highlighted Agent locations exhibiting transaction patterns or behavior that were indicative of fraud-complicity.
29. Western Union knew that the BSA required Western Union to monitor international Agents and take corrective action against Agents violating law or regulation. As a result of Western Union's willful failure to implement or execute effective global Agent disciplinary policies or to act on its employees' recommendations to discipline, suspend, or terminate international Agent locations, Complicit Western Union Agent Locations remained open for years and processed additional fraud transactions.
30. In November 2005, Western Union entered into an agreement with the Attorneys General of 47 states and the District of Columbia (the “NAAG Agreement”) to resolve the states' investigations into fraud transactions at Western Union. As part of the NAAG Agreement, Western Union promised to terminate any Agent—domestic or international—that was “complicit in fraud-induced transfers or knowingly ignore[d]

such fraud, or, if certain employees of the agent or subagent are the [*sic*] complicit or knowingly ignoring parties, insist upon termination of such employees as a condition to continued agent or subagent status.” Western Union also agreed to suspend or terminate Agents that failed to take reasonable steps to reduce fraud transactions. After entering into the NAAG Agreement, Western Union did not implement or maintain effective policies or procedures to suspend or terminate international Agents that processed fraud payments.

31. Certain Western Union employees recommended specific actions or policies and procedures to take action against potentially complicit Western Union Agent locations, but Western Union failed to adopt those recommendations. For example:
- a. Global Guidelines: As early as 2004, an employee in Western Union’s Corporate Security Department prepared a set of “draft” Global Guidelines for discipline and suspension of Western Union Agent locations worldwide that processed a materially elevated number of reported fraud transactions. In these guidelines, the Corporate Security employee proposed mandatory review of any Agent location that paid 10 CFRs within 60 days. The Corporate Security employee further proposed automatically suspending any Agent location that paid five or more transactions reported as fraud within 60 days of a review. In other words, the Corporate Security employee proposed automatically suspending any Agent location that paid 15 CFRs within 120 days. Western Union did not approve or implement the proposed Global Guidelines.
  - b. 60-Day Fraud Report: As early as 2005, Western Union’s Corporate Security Department used CFRs to generate a regular 60-Day Fraud Report, which identified Agent locations that processed five or more CFRs within 60 days. Corporate Security distributed the report to a broad group of Western Union employees, including Western Union senior employees, and cautioned that Agent locations that did not “drastically reduce” payments of transactions identified in CFRs within 60 days would be suspended. Even though Corporate Security threatened to suspend Agent locations, thousands of Complicit Western Union Agent Locations—particularly overseas—appeared on the 60-Day Fraud Report multiple times with increasing CFR payments without Western Union taking disciplinary action against them.
  - c. Agent Fraud Complicity Programs: In January 2008, two Western Union departments separately proposed methods to discipline potentially Complicit Western Union Agent Locations. One proposal specifically warned against the influence of sales employees on any Agent location disciplinary process because sales employees’ “compensation is often based on agent performance—so they ... see no reason good enough to hold their agent responsible” for fraud transactions. A Western Union senior vice president said she was “coordinating the many functions in the company that look at ... data which might indicate an agent, a location, or an agent employee is engaged in illegal activities.” She was “focused on ... analysis of the consumer fraud complaints ... from a risk-based approach, separating out agent locations ... that are complicit and need to be suspended....

[And] the need to enhance processes” at Western Union. Western Union’s then-Chief Compliance Officer wrote, “I am in favor of this proposal with two caveats: The necessary resource commitment - the more we look [for Agent involvement in fraud schemes] the more we find... and I’d like this communicated in the appropriate way so that everyone understands their roles and responsibilities.” Western Union did not implement either of the proposed disciplinary programs.

32. Had Western Union implemented the proposed Global Guidelines or the other proposed policies listed above, it could have prevented significant fraud losses to victims. Specifically, the proposed Global Guidelines would have resulted in potential suspensions and terminations against more than 2,000 Agents locations worldwide. Had Western Union implemented the proposed Global Guidelines it would have stopped these same Agent locations from processing more than \$174 million in reported fraud losses. Because few victims reported fraud to Western Union, total fraud-related losses—including reported and unreported fraud—incurred through these Agent locations is likely higher. Examples of the fraud conduct in the United Kingdom, Spain, Mexico, and Peru are below.

*The Scheme to Defraud in the United Kingdom*

33. Through its CFRs and internal reporting, Western Union was aware of dozens of Complicit Agent Locations in the United Kingdom that would have been suspended under the proposed Global Guidelines. Western Union continued to engage in business with these Agent locations and profit from their fraud transactions by, among other things, collecting fees and other revenues on each fraudulent transaction certain Complicit Western Union Agent Locations processed.
34. In 2008, Western Union owned a portion of some of the Master Agents of some of the Complicit Agent Locations. Western Union operated through Master Agent FEXCO in the United Kingdom, Spain, and other countries. Western Union owned 25% of FEXCO. FEXCO contracted with smaller independent businesses that offered Western Union money transfer services as Agent locations. Though the Agent locations in these countries did not contract directly with Western Union, Western Union could “terminate or suspend Money Transfer Services at any [Subagent location] at any time upon notice [to the Master Agent] if Western Union determine[d] in its sole discretion that operation of the Money Transfer Services at such Location(s) creates legal, regulatory, reputational, or financial risk for Western Union.” In 2008, FEXCO was Western Union’s largest Master Agent. FEXCO oversaw 10,000 Western Union Agent locations worldwide, processed more than \$4 billion in Western Union money transfer principal, and generated \$353 million in gross revenue for Western Union. Western Union Agent locations operating through FEXCO processed 89% of all Western Union transactions in the United Kingdom in 2008. As a Master Agent, FEXCO commanded commissions approximately 10 to 25 percent higher than small independent businesses that contracted directly with Western Union.
35. Western Union London Agents UK Western Union Agent 1 and UK Western Union Agent 2, which both offered Western Union money transfers in London as subagents

under FEXCO's Master Agent arrangement with Western Union, were two examples of Western Union's fraud conduct.

36. Between 2004 and 2012, UK Western Union Agent 2 appeared on more than 73 Western Union 60-Day Fraud Reports and numerous other transaction reports (e.g., the Fraud Risk Index Report). Similarly, UK Western Union Agent 1 appeared on 63 Western Union 60-Day Fraud Reports and numerous other transaction reports. Western Union received approximately 2,342 CFRs identifying more than \$3.6 million in losses to victims through fraud transactions paid by UK Western Union Agent 2 and its three related Agent locations between 2004 and 2012. During this same time period, Western Union received approximately 2,856 CFRs identifying more than \$3.6 million in losses to victims through fraud transactions paid by UK Western Union Agent 1 and its related Agent location. For years, Western Union failed to take sufficient corrective action against these high-fraud Agents.
  - a. In November 2005, Western Union's Corporate Security Department first identified UK Western Union Agents 1 and 2 in 60-Day Fraud Reports as Agents that processed a materially excessive amount of transactions reported in CFRs. Both UK Western Union Agents 1 and 2 each processed well over 15 CFRs in 120 days in 2005. UK Western Union Agents 1 and 2 appeared on every 60-Day Fraud Report in 2006.
  - b. Between January 2006 and May 2008, UK Western Union Agents 1 and 2 each appeared on the 60-Day Fraud Report repeatedly. During that time period, a Western Union Compliance analyst conducted multiple reviews of UK Western Union Agents 1 and 2 and identified suspicious activity at both Agents, which were respectively the sixth and ninth highest fraud payout Agents in the entire Europe, Middle East, and Africa region in February 2007. The analyst's findings were escalated within Western Union, but Western Union took no corrective action and instead continued business with UK Western Union Agents 1 and 2 while the Agent locations continued to process excessive amounts of reported fraud transactions.
  - c. In May 2008, a Compliance employee conducted another analysis of certain FEXCO Agents, including UK Western Union Agent 2 because "[p]revious analysis on FEXCO agents has yielded numerous compliance and fraud issues. [And t]hese issues have not been properly addressed and there is increasing interest in remediating these issues." Western Union continued to monitor these Agents, but did not terminate them as a result of the analysis.
  - d. Western Union's Board of Directors authorized Western Union to acquire the remainder of FEXCO's money transfer business for up to \$224 million in July 2008. Through the FEXCO acquisition, Western Union planned to cut commissions costs, grow its international Agent network, and increase business and revenue.

- e. At the time of the FEXCO acquisition in July 2008, certain Western Union employees including senior employees, knew that FEXCO's United Kingdom Agents had paid high levels of fraud transactions and engaged in suspicious activity since at least 2005. By July 2008, consumer fraud victims had filed 25,643 CFRs, totaling more than \$40 million in losses to victims, involving fraud paid by FEXCO Agents in the United Kingdom and Spain. This is nearly 20 percent of all fraud losses reported to Western Union from 2004—when Western Union began collecting CFRs—through July 2008. Between the time when UK Agents 1 and 2 paid 15 CFRs within 120 days and July 2008, UK Agent 2 alone paid more than \$1 million in reported fraud transactions, while UK Agent 1 paid more than \$2 million in reported fraud transactions.
- f. In advance of the FEXCO acquisition, high-level Western Union employees knew that FEXCO lowered its Agent due diligence in 2007 “because of competition they faced in the market” and that Western Union would acquire Agents “with some of the largest fraud payouts in our network” including UK Western Union Agents 1 and 2. Western Union's then-Vice President for Compliance in Europe cautioned senior Compliance employees that after acquiring FEXCO, Western Union would need to “create, almost from scratch an Agent Oversight policy and culture” at FEXCO Agents.
- g. In February 2009, Western Union acquired the remainder of FEXCO's money transfer business for a net cash purchase price of \$157.1 million. Following the acquisition, FEXCO was renamed Western Union Retail Services (“WURS”). By acquiring FEXCO, Western Union “directly manage[d]” more than 10,000 FEXCO Agent locations, including UK Western Union Agents 1 and 2. Western Union contracted directly with the former FEXCO Agents, now WURS Agents. After the acquisition and knowing that FEXCO had an ineffective AML/anti-fraud compliance program, Western Union did not suspend or terminate UK Western Union Agents 1 or 2, or other Agents that processed excessive amounts of fraud-related transfers.
- h. In November 2009, a Corporate Security employee identified high levels of fraudulent transactions paid by UK Western Union Agents 1 and 2 and other former FEXCO Agents in the United Kingdom. A Western Union Corporate Security analyst recommended to Compliance and Corporate Security employees the immediate suspension of UK Western Union Agents 1 and 2 and further warned senior employees that Agents acquired from FEXCO accounted for almost half of the fraud reports and advised that these problems “become[] our problem since we own them now.” Western Union, however, did not suspend UK Western Union Agents 1 or 2 at that time nor did it attempt to remediate the Agents.
- i. On January 15, 2010, a Compliance Analyst reviewed activity at UK Western Union Agent 1 and found “potential agent complicity in relation to fraud” that posed “significant risk to Western Union.” Despite these warnings and evidence

that UK Western Union Agent 1 was complicit in fraud, Western Union took no corrective action against UK Western Union Agent 1.

- j. On January 18, 2010, in a review of United Kingdom Agent operations, Compliance employees stated that fraud activity in the United Kingdom was on the rise and a number of Agent locations were “directly facilitating or assisting in the facilitation of fraud-related activity.” Compliance employees recommended mitigating the risk from United Kingdom Agent locations engaged in fraud “by terminating problem agents displaying common fraud patterns.”
- k. On April 29, 2010, Western Union Compliance personnel again identified activity at UK Western Union Agents 1 and 2 that “demonstrate[d] indicators of Agent complicity” in consumer fraud transactions and recommended “suspension/termination of the agent locations.” A United Kingdom employee noted that UK Western Union Agents 1 or 2 were “very high transacting locations and if they were to be deleted, there would be a huge financial loss” to Western Union. Despite U.S. Compliance’s recommendation, Western Union did not suspend or terminate UK Western Union Agents 1 or 2.
- l. About a month later, Western Union’s then-Compliance director told the then-Chief Compliance Officer and then-Deputy Chief Compliance Officer that UK Western Union Agents 1 and 2 and two related WURS Agents were four of the “six ... highest [Agents] on the fraud report for the UK.” Sales employees continued to resist full suspension or termination. In lieu of a full suspension or termination, the Compliance director reached “an agreement ... with the Business” to temporarily suspend the ability of these six Agents to pay transactions from the U.S.—though the Agents continued to process transactions, including fraud transactions, sent from outside of the U.S.—while Western Union employees had a “discussion” with the Agent owners.
- m. After a follow-up review showed that UK Western Union Agent 2 “has seen a slight decrease” in fraud complaints since the network review, Western Union lifted the suspensions after roughly three weeks and continued to conduct business with UK Western Union Agents 1 and 2 and the other Agent locations under review.
- n. Consumer fraud at UK Western Union Agents 1 and 2 returned almost immediately. On June 16, 2010, a Compliance Analyst identified UK Western Union Agent 2 as the number one paying Agent location of reported fraud in the world; that is, UK Western Union Agent 2 paid more transactions reported in CFRs between January 1 and June 15, 2010 than any other Western Union Agent. UK Western Union Agent 1 was the fifth highest CFR paying Agent during that same time period. On June 24, 2010, the United Kingdom Compliance Officer recommended terminating UK Western Union Agent 1. A senior Sales executive responded “Let’s be careful here.” Western Union did not terminate UK Western Union Agents 1 or 2.

- o. On August 13, 2010, Western Union's then-Director of Global Consumer and Agent Protection Program reviewed UK Western Union Agents 1 and 2, and other Agent locations due to a "worrysome increase" in consumer fraud payouts reported throughout the relevant region. He identified UK Western Union Agents 1 and 2, and UK Western Union Agent 2's related Agent location as "3 top bad guys" and noted that their fraud payouts were "significantly lower." Regarding some of the Agent locations, he told the then-United Kingdom Fraud Director, "You knew they were bad but not how bad! You will be surprised at how large these [consumer fraud] percentages are!" Despite the findings, Western Union did not discipline or terminate any of the three WURS Agent locations.
- p. On October 25, 2010, a Compliance manager sent the United Kingdom Compliance director and then-Regional Vice President for AML Compliance for Europe a report titled "United Kingdom Agent Complicity Review: Fraud." In his cover email with a subject of "United Kingdom – Fraud," the Compliance manager stated "things are trending up ... [Compliance] has been experiencing an increase in referrals for UK and while we have been relatively successful in keeping up with these referrals, it appears that our impact while, can be viewed as a good from a risk mitigation perspective, can also be seen as having an adverse impact on the business goals in UK....we have outlined a shift in our investigative tactics ... for UK Agents that have activity that represents likely complicity in fraud related activity. Since we have deployed these tactics, we are beginning to see that the Agents are having a hard time providing a reasonable explanation for their activity and therefore, we are seeing a number of these cases resulting in terminations."
- q. The report noted that there was "an increasing number of Western Union Agent locations [in the United Kingdom] that are either directly facilitating or assisting in the facilitation of fraud-related activity." The report stated that "a surge in UK Agent terminations due to fraud related activity in the early months of 2010" did not "permanently eliminate[]" fraud-related activity, "rather the activity had simply shifted to other locations in the same geographic areas." The report found that "locations escalated to [Western Union United Kingdom Compliance employees] were no longer being suspended and/or terminated." The report noted that an "example of this shift is the [WURS] Network" that Western Union operated directly. "WURS has agreed to the termination of only one location based on [Compliance] analysis, even though some of the most egregious levels of fraud complaints and evidence of Agent complicity have been identified at [those Agents]."
- r. In November 2010, a Compliance analyst conducted another review of UK Western Union Agent 2, and three other high-fraud United Kingdom Agent locations. The analyst again found "significant levels of questionable activity indicating Agent [or Agent employee] complicity" in consumer fraud schemes. Compliance again recommended suspension or termination of UK Western Union Agent 2 and the other Agent locations. A United Kingdom Compliance director told United Kingdom senior sales executives that "evidence of criminal or

suspicious activities from these agents seem to be rather vivid. I know some of them are the top performance [*sic*]. I will keep you posted before any action is taken.”

- s. Western Union suspended but did not terminate UK Western Union Agent 2 in November 2010. Western Union’s then-Compliance Director warned the then-Deputy Chief Compliance Officer that UK Western Union Agent 2 had been reviewed at least ten times without major disciplinary action demonstrating that “somewhere along the line, someone is losing touch with risk and is willing to absorb it.” Though Western Union temporarily suspended UK Western Union Agent 2 in November 2010, Western Union later allowed it to continue to process transactions, but temporarily restricted its ability to pay transactions of more than £350 from the United States and to send any transactions to Romania and Nigeria. While these restrictions limited the number of fraud transactions UK Western Union Agent 2 could process from U.S. victims, they did not prevent UK Western Union Agent 2 from paying fraud transfers from victims in other countries.
  - t. On December 2, 2010, a Compliance employee in the United Kingdom recommended terminating two UK Western Union Agent 2 employees but allowed UK Western Union Agent 2 to remain in operation and continue to process Western Union transactions. The Compliance employee cautioned that UK Western Union Agent 2 would be terminated if it ever appeared on Western Union’s 60-Day Fraud Report again. A few months later, UK Western Union Agent 2 appeared on Western Union’s 60-Day Fraud Report again but Western Union did not terminate UK Western Union Agent 2.
  - u. On February 2, 2011, the London Metropolitan Police contacted Western Union regarding various fraud transactions paid at UK Western Union Agent 1 and other Agents. The Compliance Director asked an employee “is [UK Western Union Agent 1] a liability?” The employee replied “it’s the same deal as [UK Western Union Agent 2] ... very high volume [Western Union Agent] that [Sales] always fights for. ... it was one of six locations suspended by [the then-Compliance Director] in May 2010 due to a high number of fraud complaints but reactivated based on negotiations with [Sales].”
37. Western Union terminated UK Western Union Agent 1 in October 2012; UK Western Union Agent 2 still operates as a Western Union Agent.

*The FTC Discussions Regarding Consumer Fraud Complicit Agents*

38. In December 2009—as fraud payouts were rising at certain Western Union Agents in the United Kingdom—the Federal Trade Commission (“FTC”) met with Western Union regarding Western Union’s antifraud efforts and the antifraud standards imposed on MoneyGram as part of the FTC’s 2009 settlement with MoneyGram. The FTC raised concerns regarding U.S. and international Western Union Agents that paid reported fraud transactions. Western Union did not adopt the standards imposed on MoneyGram.



39. After negotiating with the FTC through 2010, Western Union agreed to use an Enhanced Fraud Monitoring Process known as the “FTC Matrix” with Agents in the U.S., Canada, the United Kingdom, Jamaica, and Nigeria in April 2011. Under the FTC Matrix, Western Union told the FTC it would immediately suspend and investigate any Agent in the United Kingdom, Jamaica, or Nigeria that, within a 30-day period, processed CFR transactions comprising five percent or more of total transaction payouts.
40. Western Union’s United Kingdom Country Director told senior Compliance and Sales employees that he was “strongly opposed to the direct suspension/termination of locations [pursuant to the FTC Matrix] without any communication to the appropriate Master Agent, or the opportunity for the Master Agent to attempt to remedy the situation with the location. This could prove to be seriously detrimental to our relationship with the Master Agents. The Country Director said that the FTC Matrix would “dramatically effect [*sic*] the UK network location plan.” On April 13, 2011, a Compliance employee reported that the FTC Matrix in the “UK [was put] on hold.”
41. After discussions between Western Union Compliance Department and Sales, it was agreed that instead of suspending Agents per the FTC Matrix, Western Union would restrict certain Agents in the United Kingdom from paying transactions sent from the United States. Because most CFRs were made by U.S. consumers, transactions identified in CFRs almost always originated from the U.S. As a result, restricting certain United Kingdom Agents from paying transactions originating in the U.S. meant that those Agents could not process transactions identified in CFRs and therefore would not hit the FTC Matrix.
42. The U.S. transaction restriction was not effective at combating fraud. As one Western Union employee explained to Western Union’s United Kingdom Compliance Officer on June 8, 2011, “Problem is, we agreed in writing with the FTC on how to handle this stuff ... Suspend pending was in the agreement. Also what I don’t like about just blocking US to UK is that we aren’t addressing potential bad Agents that way. People around the world are being defrauded but we only have data on the sends from the US though.”
43. Western Union told the FTC about its restriction of certain Agent locations in the United Kingdom in summer 2012.

*The Scheme to Defraud in Spain*

44. As with the United Kingdom, Western Union operated in Spain through Master Agent FEXCO. FEXCO contracted with subagents in Spain to process transactions, with FEXCO subagents processing 40% of all Western Union transactions in Spain in 2008. When Western Union acquired FEXCO’s money transfer business in February 2009, it entered into direct relationships with all of FEXCO’s subagents in Spain.
45. In 2010 and 2011, Compliance employees identified Agent locations in Spain processing increasing numbers of reported fraud transactions. Between 2008 and 2010, reported fraud activity in Spain increased by a factor of eight. In 2008, victims filed 252 CFRs with Western Union regarding fraud transactions paid by Western Union Agent locations

in Spain totaling \$379,986 in losses to victims. In 2010, victims filed 2,192 CFRs with Western Union regarding fraud transactions paid by Western Union Agent locations in Spain totaling \$5,127,420 in losses to victims.

46. On January 21, 2011, Western Union Compliance employees conducted a “Spain Fraud Review” for “Agent Complicity.” Compliance employees found that CFR transactions paid in Spain drastically increased throughout 2010 and the estimated levels of total fraud paid by Agent locations with questionable activity “were often more than five times that of [CFR] figures associated with each” Agent location. Agents Western Union directly managed after it bought FEXCO were the “majority” of the Agents that demonstrated “complicity related to fraudulent activity.” A then-Compliance manager recommended to Compliance and Fraud Department vice presidents that Western Union take action against certain Agents.
47. The report continued “in addition to suspending or terminating several locations, [Western Union Regional Compliance has] also worked with Agent Networks to address issues identified by [Compliance]. Some of the actions taken include temporarily routing Pay transactions through Agent CSCs for screening prior to payout. Additionally, Agents have in some cases limited the amount of Pay transactions particular locations can process in a given time period.” The report stated that “these controls have in some instances helped to reduce the amount of fraudulent activity occurring at locations in Spain.” The report concluded that Compliance “investigations continue[d] to identify levels of potential fraud that far surpass figures demonstrated by formal fraud complaints suggest[ing] high levels of risk related to Agent Complicity and fraudulent activity in the country. Additionally, the increasing trend of fraud complaints throughout 2010 indicates that the number of Agents appearing on the FRI will continue to increase and the number of Agent locations identified that display indicators of Agent complicity will likely surpass the number discovered in 2010, thus further heightening the risk exposure to Western Union.”
48. On August 18, 2011, the Compliance Director and Compliance Managers recommended to the Director of Global Consumer and Agent Protection Program that Western Union address rising fraud in Spain by adding Spain to the FTC Matrix. Western Union did not follow Compliance’s recommendation. Fraud transactions continued to increase in Spain throughout 2011. In 2011, victims filed 3,710 CFRs with Western Union regarding fraud transactions paid by Western Union Agents in Spain totaling \$7,593,352 in losses to victims.
49. In 2011 and 2012, SEPBLAC, Spain’s Anti-Money Laundering and Countering Financing of Terrorism Supervisory Authority, conducted an audit of Western Union’s Agents in Spain that revealed money laundering and fraud activity at certain Western Union Agent locations in Spain. In a report dated October 9, 2012, SEPBLAC informed Western Union that its work “reveals extremely serious facts.” SEPBLAC noted that, for a percentage of certain Western Union Agent locations, Western Union “itself has reported in suspicious transaction reports ... [that] there were clear signs that [certain Agent locations] carried out money laundering activities.” SEPBLAC found that the money laundering activity was “particularly remarkable in overseas remittance

transactions to Spain.” SEPBLAC determined that certain Agent locations “feign[ed] the involvement of beneficiaries who do not really exist, that is to say, the payments are not collected by clients, but by [A]gents who use an identity invented for that purpose.” SEPBLAC found that Western Union “reported to the Executive Service a significant numbers of [Agents] and cancelled the corresponding agency contracts.” Nevertheless, SEPBLAC concluded that Western Union’s “money laundering and terrorism financing prevention systems [were] ineffective” and due diligence was deficient.

50. In a report dated December 20, 2012, SEPBLAC concluded that Western Union had not “fully accepted” the seriousness of the conduct SEPBLAC identified in its October 9, 2012 report, and that Western Union’s response to the October 9 findings, which stated that the report “indicated some needs for improvement in the agent oversight program” minimized what was an “absolute lack of control over the [A]gents’ activity which has made it possible for truly scandalous figures of fraud and money laundering related payments and remittances to be recorded.” On December 20, 2012, SEPBLAC found Western Union’s AML system in Spain “totally ineffective in preventing money laundering, related to fraud and other offenses, which has taken place on a large scale.”

*The Scheme to Defraud Elsewhere*

51. Western Union knew that Complicit Western Union Agent locations were not limited to the United Kingdom and Spain, but failed to implement or execute effective world-wide fraud policies until September 2012, eight years after employees first recommended adopting global policies.
52. As early as March 2011 and continuing through 2012, certain Complicit Western Union Agent Locations in Mexico conspired to launder fraud proceeds using Western Union’s Money Transfer System. In these schemes, Complicit Agent locations in Mexico received the initial fraudulent transactions from victims in the United States via Western Union’s Money Transfer System. Minutes later, after taking a commission, the Complicit Agent Locations in Mexico would use the Western Union Money Transfer System to send the remaining money to Western Union Agent locations in Canada and other destinations. This two-step process was designed to conceal the ultimate destination of the fraud proceeds. Despite identifying certain Agent locations potentially involved in this activity as early as April 2011, Western Union allowed the Agent locations to remain open and the activity continued through 2012.
53. In October 2011, Western Union learned from U.S. law enforcement and its own review of transaction data that certain Agent locations in Peru were participating in an emergency need fraud scam. Western Union reviewed four related Agent locations in Peru and found that those four Agent locations paid nearly half of all CFR transactions paid in Peru. Western Union did not terminate the Agent locations in October 2011, but instead allowed them to continue processing transactions. In the next six months, one of the four Agent locations paid 250 more CFR transactions totaling more than \$600,000. Western Union suspended the four Agent locations in April 2012, but allowed the Agent locations’ owner to open another Western Union Agent location nine months later.

*Victims of the Scheme to Defraud*

54. Below are examples of victims of the consumer fraud scheme perpetrated via Western Union's Money Transfer System. Each of these victims was defrauded through Agents that had already paid 15 CFRs in 120 days.
- a. MV, a 60-year-old resident of the Middle District of Pennsylvania reported that in February 2006, a Fraudster contacted MV and falsely promised him that if he paid legal fees up front, he would receive a \$1 million prize. On February 2, 2006, MV visited a Western Union Agent location in the Middle District of Pennsylvania and sent a \$4,500 money transfer to claim his prize. UK Western Union Agent 2 in London, United Kingdom paid MV's transfer on February 3, 2006. MV never received the prize he was promised.
  - b. AI, a resident of the Middle District of Pennsylvania reported in July 2006, a Fraudster contacted AI and falsely promised her that if she paid money up front she would receive a sweepstakes prize. On July 8, 2006 and July 14, 2006, AI visited Western Union Agent locations in the Middle District of Pennsylvania and sent transactions of \$1,500 and \$1,750 to claim her prize. On July 10, 2006 and July 15, 2006, UK Western Union Agent 2 in London, United Kingdom, paid out AI's transfers. AI never received the prize she was promised. AI reported the fraud to Western Union.
  - c. TD, a resident of the Middle District of Pennsylvania reported in May 2008, a Fraudster contacted TD and falsely promised him a motorcycle in exchange for an advance payment. On May 29, 2008, TD visited a Western Union Agent location in the Middle District of Pennsylvania and sent a \$1,300 money transfer in exchange for the motorcycle. On May 31, 2008, UK Agent Western Union 2 in London, United Kingdom, paid out TD's transfer. TD never received the motorcycle he was promised. TD reported the fraud to Western Union.
  - d. FS, a resident of the Middle District of Pennsylvania reported in May 2010, a Fraudster contacted FS and falsely promised to pay him for cashing checks provided FS paid the Fraudster the value of the checks in advance. On May 19, 2010, FS visited a Western Union Agent location in the Middle District of Pennsylvania and sent a \$2,000 money transfer to receive the checks. UK Western Union Agent 1 in London, United Kingdom paid FS's transfer on May 20, 2010. The checks FS received were counterfeit and FS never received the payment he was promised. FS reported the fraud to federal investigators.
  - e. PM, a 65-year-old resident of the Middle District of Pennsylvania reported that in May 2010, a Fraudster contacted PM and falsely promised her that if she paid fees up front she would receive prize money from a sweepstakes. Between May 1, 2010 and September 15, 2010, PM visited a Western Union Agent location in the Middle District of Pennsylvania and sent seven Western Union transactions totaling \$9,550 to claim the prize. A Western Union Agent in London, United Kingdom, paid three of PM's transfers totaling \$3,450. PM never received the

sweepstakes prize she was promised. PM reported the fraud to federal investigators.

- f. MSC, a 90-year-old resident of the Middle District of Pennsylvania reported that in June 2011, a Fraudster contacted MSC and falsely told her that a family member was in trouble and needed monetary assistance. On June 24, 2011, MSC visited three different Western Union Agent locations in the Middle District of Pennsylvania and sent four money transfers totaling \$9,600 to help her family member. On June 24, 2011, two Western Union Agent locations in Spain paid two of MSC's transfers and a Western Union Agent location in Mexico paid two of MSC's transfers. MSC's family member was never in trouble and did not need monetary assistance. On July 29, 2011, MC reported to Western Union that she had been the victim of a fraud. Western Union recorded only one of MSC's four transactions in its CFR database.
- g. KL, an 85-year-old resident of the Middle District of Pennsylvania reported that in August 2011, a Fraudster contacted KL and falsely told him that a family member was in trouble and needed money. On August 11, 2011, KL visited a Western Union Agent location in the Middle District of Pennsylvania and sent two money transfers totaling \$12,000 to help his family member. On August 11, 2011, two Western Union Agent locations in in Mexico paid KL's transfers. KL's family member was never in trouble. KL reported the fraud to Western Union.
- h. TSD, an 82-year-old resident of the Middle District of Pennsylvania reported that in August 2011, a Fraudster contacted TSD and falsely told him that a family member was in trouble and needed bail money. On August 18, 2011, TD visited a Western Union Agent location in the Middle District of Pennsylvania and sent a \$2,300 money transfer to help his family member. On August 18, 2011, a Western Union Agent location in Spain paid TSD's transfer. TSD's relative was never in trouble. TSD reported the fraud to Western Union.
- i. RK, an 80-year-old resident of the Middle District of Pennsylvania reported that in August 2011, a Fraudster contacted RK and told her that her grandson was in an accident and needed money. On September 6, 2011, RK visited a Western Union Agent location in the Middle District of Pennsylvania and sent two transfers totaling \$9,800 to help her grandson. On September 6, 2011, a Western Union Agent location in Mexico paid both of RK's transfers. RK's grandson had not been in an accident. RK reported the fraud to Western Union.
- j. JD, an 88-year-old resident of the Eastern District of Pennsylvania reported that in October 2011, a Fraudster contacted JD and falsely told him that his grandson was in the hospital and needed money. On October 4, 2011, JD visited a Western Union Agent location in the Eastern District of Pennsylvania and sent a \$2,200 money transfer to help his grandson. On October 4, 2011, Western Union Agent location in Spain paid JD's transfer. JD's relative was never in the hospital.

- k. MC, a resident of the Southern District of Florida reported that on February 15, 2012, a Fraudster contacted MC and falsely told him a relative was in trouble and needed money. Between on or about February 15, 2012 and February 17, 2012, MC visited five Western Union Agent locations in the Southern District of Florida and sent five transfers totaling over \$10,000. A Western Union Agent location in Peru paid three of MC's transfers on or about February 16, 2012. MC's relative had never been in trouble. MC reported the fraud to Western Union.
- l. HH, a 96-year-old resident of the Middle District of Pennsylvania reported that in February 2012, a Fraudster contacted HH and falsely told him that his grandson had been arrested abroad and needed bail money. On February 27, 2012, HH visited a Western Union Agent in the Middle District of Pennsylvania and sent two \$2,400 money transfers to help his grandson. A Western Union Agent location in Peru, paid HH's transfer on February 27, 2012. HH's grandson had not been arrested and did not need bail money. HH reported the fraud to Western Union.

**Western Union's Willful Failure to Prevent Structuring**

- 55. In March 2003, FinCEN fined Western Union \$3 million, finding that the Company willfully failed to file SARs and "failed to establish SAR reporting procedures that would reasonably assure that it could identify and properly report structured transactions." As part of the penalty, Western Union agreed to conduct further review to identify suspected structuring to avoid the CTR or \$3,000 identification requirements and to "establish an enhanced nationwide due diligence policy to monitor its agents for BSA compliance [, which] shall include ... terminating such agents that Western Union determines to be in chronic violation of Western Union policies and/or a substantial risk for money laundering."
- 56. Between 2004 and 2012, Western Union failed to terminate or discipline certain Agent locations who sent a high volume of transactions from the U.S. to China ("China Corridor Agents") and repeatedly violated the BSA and Western Union policy through their structuring activity.
- 57. As described in more detail below, Western Union, through various methods, recognized that four China Corridor Agents were engaged in violations of Western Union policies regarding structuring transactions. Western Union tracked how many SARs it filed on its Agent locations' transactions and knew that a high number of SARs on transactions at a particular Agent location was an indicator that the Agent location might be involved in suspicious or illegal activity. Western Union filed thousands of SARs identifying individuals who sent potentially structured transactions through the China Corridor Agents. Between 2003 and 2012, Western Union filed more than 11,000 SARs on transactions conducted at one of the China Corridor Agents, U.S. Shen Zhou International Company, and more than 20,000 SARs on transactions conducted at three other China Corridor Agents, collectively.

58. Some Western Union employees encouraged China Corridor Agents to grow their business by urging Agent owners to open additional Western Union locations and paying the owners bonuses. Some Western Union employees also pressed Compliance employees to ensure that certain China Corridor Agent locations were not suspended or terminated.
59. Although Western Union filed thousands of SARs on customers of its Agent locations, Western Union rarely identified its Agent locations as suspicious actors or described the Agent locations' role in the structuring conduct. Western Union's practice was not to identify Agent locations as "subjects" of SARs unless Western Union found an Agent location "complicit" and terminated the Agent location as a result of the finding. Western Union typically only found Agent locations "complicit" if the owner or employee of an Agent location was arrested or identified in a public source such as "a news article that says the [Agent was] related to fraud, or [the Agent] was on ... some sort of scam website" or if its own investigation determined that the Agent location was complicit.
60. Between 2004 and 2012, customers at certain China Corridor Agents structured hundreds of millions of dollars in Western Union transactions to China. These China Corridor Agents were highly profitable and sent transactions from the U.S. to China between 2003 and 2012. Had Western Union's AML program been effective, Western Union could have prevented these four Agent locations from allowing customers to structure at least \$64 million of transactions beginning as early as April 2009.

*U.S. Shen Zhou International Company*

61. U.S. Shen Zhou International Company ("USZ") was a vitamin and herbal supplements store owned by Frank Wang and located in Monterey Park, California in the Central District of California. On March 24, 2005, Wang became a Western Union Agent. USZ sent more than ninety percent of its transactions between 2005 and 2010 to China. USZ quickly became one of the largest Independent Western Union Agent locations in the United States, processing more than 100 Western Union transactions per day. By April 26, 2006, a Western Union sales employee described USZ as the "#1 China account." Between 2005 and 2010, USZ sent more than \$310 million in Western Union transactions to China, approximately 50 percent of which were structured.
62. Wang pleaded guilty to illegal structuring in the U.S. District Court for the Central District of California on October 25, 2013. According to Wang, he and his employees at USZ structured and aided consumers in structuring a significant volume of Western Union transactions from the U.S. to China. Wang said that he and his employees allowed and assisted consumers in structuring transactions to avoid the BSA requirement that financial institutions review and record consumer identification on transactions of \$3,000 or more. In aiding consumers in structuring these transactions, Wang said he supplied false identity information for his customers and entered that false information into Western Union's Money Transfer System. Wang admitted to the Court that he acted in part to benefit Western Union by increasing revenue from fees to Western Union.

63. Western Union employees knew that Wang and USZ employees were potentially structuring or aiding consumers in structuring transactions in violation of the BSA as early as December 2005, but allowed USZ to continue operating and sending structured transactions using Western Union's Money Transfer System until Wang was arrested in October 2010.
64. Between December 2005 and March 2010, Western Union conducted at least nine onsite compliance reviews at USZ and dozens of transaction reviews. In each onsite review, Western Union Compliance employees found that USZ employees were failing to comply with elements of the BSA or certain aspects of Western Union policy. Western Union repeatedly found that USZ was deficient in monitoring transactions, was not filing CTRs on all transactions that should have triggered the filing of a CTR, and was processing suspicious transactions without filing SARs on those transactions. The suspicious transactions were unusual and "repetitive," characterized by multiple transactions of \$2,500 each sent minutes apart, indicated that consumers were likely structuring transactions to avoid providing identification as required by the BSA.
65. Between 2005 and March 2010, despite finding repeated violations of Western Union policies, Western Union took no disciplinary action against USZ beyond one 90-day probation in January 2006 during which USZ continued to process transactions.
66. For example, in March 2010, Western Union conducted a compliance review of USZ that revealed failures to file SARs and verify customer identities. Under Western Union's compliance policies, USZ's failures should have resulted in Western Union placing the Agent on a 90-day Compliance Probation. Western Union did not place the Agent on probation, instead—contrary to its compliance policies—Western Union continued to monitor the Agent's transactions.
67. By 2010, Western Union had filed more than 11,000 SARs regarding transactions sent through USZ, without identifying USZ or Wang as individuals involved in suspicious conduct. The vast majority of the SARs Western Union filed identified the suspicious activity as structuring to avoid the BSA identification recordkeeping or CTR reporting requirements. Despite repeatedly finding that USZ was not complying with all elements of the BSA or all elements of Western Union's AML requirements, Western Union did not identify the Agent's suspicious conduct in the SARs it filed with law enforcement nor did it take any material action to stop USZ from assisting third parties in using Western Union systems to send structured transactions.
68. On September 27, 2010, Wang was arrested for structuring through USZ. Western Union terminated USZ as an Agent after Wang's arrest. After Wang's arrest, he told law enforcement that a Western Union sales employee told Wang that Wang could open another Western Union Agent location in the Monterey Park, California area. The Western Union employee cautioned Wang not to use his own name to open the new Agent location, but to use a relative's name instead. Wang did not open another Western Union Agent location.



*Two China Corridor Agents in New York*

69. New York Agent 1 and New York Agent 2 were phone card and phone accessories stores owned and operated by Owner 1 in New York, New York. In 2003, Owner 1 began operating New York Agent 1 as a Western Union Agent location; Owner 1 began operating New York Agent 2 as a Western Union Agent location in 2005. Both Agents were “direct deposit” Agents, which means that they banked under Western Union’s name and were meant to receive additional review under Western Union’s policies. Between 2003 and 2011, New York Agents 1 and 2 sent more than \$1.6 billion in Western Union transactions; almost all of those transactions were sent to China and approximately 25 to 30% of those transactions had characteristics indicative of structured transactions.
70. New York Agents 1 and 2 were China Corridor Agents located in New York and both Agent locations became two of the largest Western Union Agent locations in the U.S., with New York Agent 1 processing approximately 3,000 transactions each month and New York Agent 2 processing approximately 5,000 transactions each month. One then-executive vice president noted that “any negative action against [New York Agent 1] will require prior notification” to Western Union’s then-President for the Americas and then-Executive Vice President for Asia Pacific “due to the heavy impact to our China business.”
71. Owner 1 admitted to government law enforcement agents that he knew that consumers paid their debt to human smugglers in China through Western Union and that consumers would keep transactions under \$2,000 in order to avoid providing identification.
72. Western Union employees knew through compliance reviews, transactions reviews, and automatic reports designed to identify suspicious activity that New York Agent 1 and 2 employees were potentially structuring or aiding consumers in structuring transactions in violation of the BSA as early as 2006. For example, between 2004 and 2011, Western Union conducted at least a dozen onsite reviews of New York Agent 1 and eight onsite reviews of New York Agent 2. In each review Western Union found that the employees of New York Agents 1 and 2 were not complying with certain elements of the BSA or Western Union policy. Western Union repeatedly found that New York Agents 1 and 2 did not have sufficient compliance programs, were not filing SARs in every instance when a SAR was required, were allowing consumers to allegedly structure transactions, and were, in certain instances, entering false data in Western Union’s Money Transfer System.
73. Despite these repeated violations, Western Union continued business with New York Agents 1 and 2 and allowed the Agent locations to continue operating and sending structured transactions using Western Union’s Money Transfer System until a bank asked Western Union for more information on the Agent locations’ AML programs in November 2011. Instead of suspending or terminating the Agent locations, Western Union permitted these Agent locations to continue operating. For example:

- a. Western Union had an unwritten policy to suspend an Agent location from conducting transactions if that Agent location was placed on probation three times. The term “probation” referred to Western Union’s policy of engaging in enhanced reviews of an Agent location. On July 18, 2008, a senior Compliance Officer noted that New York Agent 1 had been placed on probation by Western Union on three occasions but was not suspended per Western Union policy. Western Union approved New York Agent 1’s owner to open a third Agent location and paid the owner a \$250,000 bonus to renew New York Agents 1 and 2’s contracts with Western Union.
- b. In November 2008, a Compliance employee recommended New York Agent 2’s third probation. Several months later a Western Union Sales employee stated that Sales was “encouraged to be proactive” with Agent locations with more than “2 ‘bad’ reviews. [Because i]f the agent has a third it is automatic suspension, no appeal and the recovery process takes about a week... Attitude seems to be a key portion of the process. If the agent is resistant rather than willing to adopt changes then they head very quickly to suspension.” A Western Union Sales director responded that Sales “help compliance group understand how important those Chinese agents are – not to shut them down automatically. [New York Agent 2] is #2 agent in the region and we can’t afford one week suspension.”
- c. On June 3, 2010, Western Union’s then-Compliance Director told the then-Chief Compliance Officer that Western Union reviewed New York Agent 1 on June 2, 2010. New York Agent 1 “had a bunch of transactions with false data[.] The [New York Agent 1 Compliance Officer, who was also the owner’s sister] admitted to accepting a bag of cash (80K) from a relative and making up transactions ... So, the [Compliance Officer] of one of our biggest locations knew that she was breaking the law. This, plus other findings (forms did not match what was entered into the system) puts this as a suspension [of New York Agent 1]. This would be the [Agent’s] third compliance suspension. If I don’t suspend, then it is a probation. This would be [New York Agent 1’s] third probation, which is also a suspension. I’ll call the [Western Union] Business [employees].”
- d. Sales employees raised concerns with this suspension. Western Union’s then-President of the Americas told Western Union’s Chief Executive Officer “FYI. We are trying to save [New York Agent 1] (to [sic] agent NY to China).” Compliance suspended New York Agent 1 on June 3, 2010, but lifted the suspension 24 days later. New York Agent 1’s Compliance Officer continued to process transactions for another year despite admitting that the Compliance Officer conducted criminal transactions. Subsequent, Western Union compliance reviews continued to uncover additional BSA violations.
- e. A review of New York Agent 1 on November 12, 2010, revealed serious compliance failures, including violations of the BSA’s recordkeeping and reporting requirements that caused Compliance to recommend the Agent location’s third probation, which should have resulted in the Agent location’s immediate suspension. Avoiding probation and suspension for the Agent location

“require[d] a policy exception” from a Compliance employee. Western Union employees did not suspend New York Agent 1 after this review.

- f. After a review of New York Agent 1 in January 2011, a Compliance employee again recommended suspension due to New York Agent 1’s continued compliance failures. Compliance suspended New York Agent 1 briefly but “after discussions with the business” placed New York Agent 1 on an *Enhanced Probation Program*” that allegedly would have included “full training initially and then monthly, unannounced visits by [Western Union]”.
74. In 2011, the bank that held New York Agents 1 and 2’s direct deposit accounts asked Western Union to provide information about the compliance programs, risks, and reviews related to Western Union Agent locations who used the direct deposit accounts, including New York Agents 1 and 2. A Western Union Compliance employee said that if the bank found that “the risk is high, they may pull some of the bank accounts for these [Agents], which effectively will result in suspension of services. [The bank] can also file its own SARs and conduct law enforcement outreach which can elevate the risk that Western Union has with these locations.”
75. The compliance employee also told other Compliance employees that he was communicating with the bank about the Agent locations, and that the other employees should “prepare [Sales] for this should it get to a point where [the bank] pulls a few bank accounts. I intend to communicate the significant amount of resources that Western Union puts towards maintaining these locations and will even demonstrate that we will terminate as we did with [another Agent location].” In November 2011, the bank asked for additional compliance information on New York Agents 1 and 2, and other Agent locations, including any material findings regarding the Agent locations. Western Union shared none of its findings regarding either New York Agents 1 or 2 with the bank. A senior Western Union sales executive told colleagues that closing “[New York Agents 1 and 2] at this time will impact the US-China corridor BADLY. Please see if there is anything we can do (like verify [New York Agent 1] has done something ‘not compliant’ and we re-educate [New York Agent 1] to be compliant) and to re-open them in a few weeks to catch the Chinese New Year rush.”
76. Following the bank’s requests for information, Western Union closed New York Agents 1 and 2 in December 2011.
77. By 2012, Western Union had filed nearly 20,000 SARs regarding transactions sent by New York Agents 1 and 2. Despite Western Union’s earlier findings, only two of these SARs identified the Agent’s involvement in suspicious activity. Between 2005 and 2012, the vast majority of these SARs identified the suspicious activity as structuring to avoid the BSA identification recordkeeping or CTR reporting requirements.

*Hong Fai also known as Yong General*

78. Hong Fai General Contractors Corp., which later changed its name to Yong General Construction Co. Inc. (“Hong Fai”) was a construction company owned by Yong Quan

Zheng<sup>1</sup> located in Philadelphia, Pennsylvania in the Eastern District of Pennsylvania. On September 13, 2006, Zheng signed an agreement to operate Hong Fai as a Western Union Agent from the small construction company office in the Chinatown area of Philadelphia. Zheng's daughter Yan Hong Zhao a/k/a Yan Hong Zheng a/k/a Cindy ("Cindy") and son-in-law Ming Zhao a/k/a Larry ("Larry") operated the Western Union business at Hong Fai. Hong Fai quickly became a successful Western Union Agent location, processing more than \$100,000 in money transfers per day, most of which were sent to China, by February 2007. From December 1, 2007 through March 6, 2012, Hong Fai sent over \$126 million in Western Union transactions.

79. On October 18, 2016, Cindy and Larry were charged in the U.S. District Court for the Eastern District of Pennsylvania with conspiracy to violate the BSA, including structuring of at least \$21 million of transactions to China, and failure to file SARs. Sentencing for both defendants is scheduled for March 2017.
80. Western Union employees knew that Hong Fai employees structured or aided or were potentially structuring or aiding consumers in structuring transactions in violation of the BSA and that Hong Fai was not filing SARs as required, but allowed Hong Fai to continue operating and sending structured transactions using Western Union's Money Transfer System. As described below, through compliance reviews and other methods, certain Western Union employees identified suspicious and illegal conduct at Hong Fai for years but did not follow Western Union's internal procedures to discipline or terminate Hong Fai.
81. For example, between 2007 and 2012, Western Union conducted more than a dozen onsite or transaction reviews of Hong Fai. In these reviews, Western Union repeatedly found that Hong Fai violated certain elements of the BSA or certain aspects of Western Union policy. These reviews resulted in Western Union placing Hong Fai on probation three times, which should have resulted in suspension per Western Union practice. Despite these repeated violations, Western Union continued business with Hong Fai without effective discipline and allowed Hong Fai to change its name to Yong General and receive a new Agent identification number, which made it appear as though it was a new Agent location. Despite continued violations under its new name, Western Union terminated Hong Fai in 2012 only after law enforcement and Hong Fai's bank continued to raise concerns about illegal transactions and Hong Fai's failure to file SARs. Western Union filed no SARs identifying Hong Fai as a suspicious subject until after it terminated Hong Fai in 2012.
82. As early as June 2007, Western Union was aware of "significant" compliance failures at Hong Fai involving structured transactions and failure to file SARs for suspicious transactions, but allowed Hong Fai to continue to operate. During a March 2008 review, a Compliance employee determined that the Agent location was structuring to avoid identification and CTR requirements, and also had failed to file SARs on suspicious transactions. As early as January 2009, Hong Fai's bank notified Western Union that Hong Fai was engaged in suspicious transactions based on suspicious patterns of Hong

---

<sup>1</sup> Yong Quan Zhen pled guilty to unrelated charges on May 31, 2016.

- Fai's deposits and reports from third parties. Western Union allowed Hong Fai to remain in operation.
83. On March 29, 2009, Western Union Compliance employees tried to suspend Hong Fai after Larry, who conducted the majority of transactions, told Western Union employees "he [was] not willing to comply with the AML Laws and Policies." The compliance review also found that Hong Fai failed to file SARs on suspicious transactions, and Hong Fai employees were "helping customers structure transactions to avoid 3K [BSA] ID" requirement, a violation of the BSA.
  84. Western Union Compliance scheduled the start of Hong Fai's suspension for April 9, 2009. Sales employees requested a delay in suspension because Hong Fai was a "very important Agent." Despite the results of the compliance review showing that Hong Fai was violating the BSA, including structuring, after discussions with Sales, Compliance suspended Hong Fai, but within a few days lifted the suspension and rather placed it on probation and allowed the Agent location to continue processing transactions.
  85. Hong Fai's compliance failures continued in 2010, when law enforcement contacted Western Union again about potential illegal payments sent through the Agent location. Compliance employees reviewed Hong Fai's compliance history and found Hong Fai had multiple compliance failures dating back to 2007 that included structuring conduct and failure to file SARs, and that Hong Fai's failures were continuing to take place. On June 10, 2010, Western Union's Compliance Manager shared Hong Fai's March 2009 compliance review with his team. A Compliance analyst responded that Hong Fai's suspension had been changed to probation after Sales told Compliance that Hong Fai was the highest performing U.S.-to-China Agent in the Philadelphia region.
  86. In November 2010, a Compliance employee recommended discussing suspension of Hong Fai as "their compliance issues have not been resolved and the agent owner is sending transactions using different biographical data." A compliance review on November 18, 2010, revealed that the owner was sending Western Union transactions for himself from the U.S. to China with false data. A Compliance employee warned "if this [A]gent is willing to enter different biographical information on transactions they are conducting for themselves, it is logical to conclude that they would be willing to enter fictitious biographical information for another consumer." As part of this report, a Compliance employee noted that "Hong Fai ... pose[d] significant consumer, legal/regulatory, financial and reputational risk to Western Union ... evidenced by the questionable consumer traffic, questionable agent activity, and the Agent's inability to adhere to compliance standards." Nevertheless, Western Union did not suspend this Agent location.
  87. An onsite compliance review in July 2011 revealed continued violations of the BSA and Western Union policies. During the review, Cindy admitted to a Western Union Compliance employee that she would have structured a consumer's \$14,000 transaction into two transactions of less than \$10,000 each if the Western Union employee had not been present because "good customer service was more important than compliance." The Western Union Compliance employee also observed Hong Fai employees advising

consumers on how to structure transactions, charge extra fees for transactions, and accept transactions over the phone. Hong Fai consumers told the Western Union Compliance employee that they had been able to use false identification documents at Hong Fai in the past.

88. Western Union did not suspend or terminate Hong Fai in 2011 though a then-Compliance director told a then-Compliance vice president that Western Union “[has] taken a huge chunk out of the US to China business this week by suspending 8 locations, 6 in the [Southwest Border] area and 2 in New York. We should have had another in Philly, but we’ve opted to let [Global Field Compliance] apply iCop.” The employee stated “as soon as its [sic] possible, we should apply RTRA controls on all US to China transactions.” The same then-Compliance director explained that though he was considering termination for Hong Fai in 2012, Sales had always “wanted this [Agent] saved and I don’t think anything has changed in their minds around the importance of the [A]gent.”
89. On March 19, 2012, Western Union terminated Hong Fai as an Agent. Between 2007 and 2012, Western Union filed more than 1,000 SARs on transactions Hong Fai processed.

#### **AML Deficiencies Involving Gambling Transactions at Western Union**

90. In December 1997, Western Union signed an Agreement of Voluntary Cooperation with the Florida Attorney General regarding gambling transactions from Florida to offshore sportsbooks. As part of the agreement, Western Union agreed to advise certain Agents that interstate wagers violated Florida law and to implement procedures to limit certain gambling transactions.
91. Through transaction data, Agent compliance reviews, additional law enforcement investigations, and other investigations, Western Union employees knew that individuals located in the Southern District of Florida and elsewhere continued to use its Money Transfer System through at least 2012 to send transactions that exhibited characteristics Western Union associated with illegal gambling-related transactions from the U.S. to other countries. Western Union detected these transactions in its Money Transfer System and knew that gambling-related transactions were “particularly well-suited for the layering and integration stages of money laundering. As a result, gambling websites generate substantial money laundering concerns due primarily to the volume and speed of transactions, as well as the anonymity offered. For these reasons, internet gambling operations are vulnerable to be used, not only for money laundering, but also for criminal activities ranging from terrorist financing to tax evasion.” Western Union employees identified legal and regulatory risks to Western Union if U.S. law enforcement found that the Company had “knowingly processed transactions for the purpose of illegal gambling.”
92. Although Western Union had some systems and controls in place to combat the use of Western Union’s system to transmit illegal gambling-related transactions, Western Union did not enact effective controls to limit transactions that displayed characteristics

associated with gambling through 2012. For example, in August 2009, Western Union Compliance employees proposed enhanced consumer monitoring on transactions from the U.S. to Costa Rica to reduce transactions that exhibited characteristics associated with gambling. Under the proposal, any consumer who sent a certain number of transactions exceeding a certain amount within a certain period would be subject to additional review and, if warranted, blocked from sending further Western Union transactions.

93. Western Union implemented the enhanced consumer monitoring, but the monitoring did not reduce or eliminate gambling-related transactions sent by U.S. consumers to Costa Rica, which U.S. consumers sent “to take advantage of the many Costa Rican based gaming websites operating in the country.” For example, between January and February 2010, a Western Union analyst reviewed certain Agents in Costa Rica and found that “even with controls in place and additional requirements placed on our Agent Networks, the transaction patterns are indicative of Agent Complicity” in the gambling transactions. A Western Union analyst also found that the “enhanced consumer monitoring program [implemented in 2009] has not been effective in lessening the questionable activity (likely related to gaming) being sent from the U.S. to Costa Rica.” The analyst proposed additional controls on Agents in Costa Rica including limiting the Agents to specific but confidential payout thresholds.
94. By at least July 2010, Western Union Compliance, Sales, and Technology employees began to discuss using Real Time Risk Assessment (“RTRA”) controls to limit transactions with characteristics associated with gambling from the U.S. to Costa Rica. In August 2010, Western Union concluded that the proposed RTRA rule would impact 18 Agents in Costa Rica and affect approximately \$1 million worth of money transfers per month. Though Compliance employees pressed to get RTRA implemented due to ongoing identification of gambling-related transactions between the U.S. and Costa Rica, by October 2010, Western Union had not implemented this specific RTRA control targeting off-shore gaming.
95. On October 14, 2010, Western Union Compliance analysts conducted another review of transactions paid by certain Agent locations in Costa Rica. The analysts interviewed some consumers who sent the transactions and admitted they were funding their online gambling accounts for the website [www.pokerstars.com](http://www.pokerstars.com). The analysts found continued questionable Agent activity at certain Agent locations in Costa Rica which indicated that Agent location employees allowed some customers to provide incomplete or false information to receive suspicious transactions.
96. On November 23, 2010, Compliance employees concluded that the enhanced consumer monitoring program was “not covering the appropriate risk and thus not as effective as it could be.” Compliance employees decided to suspend the program.
97. On December 10, 2010, Compliance employees shared a plan with business employees for RTRA controls designed to reduce gambling-related transactions. Compliance employees noted that many consumers who confirmed that their transactions to Costa Rica were “for gambling purposes” sent multiple transactions within 30 days. According to Compliance employees, the enhanced consumer monitoring program did “not appear

to be decreasing the amount of questionable transactions being paid out in Costa Rica.” Compliance proposed automatically limiting U.S. consumers to sending a specific number of transactions at specific thresholds to Costa Rica within a calendar month. Western Union implemented the RTRA program in March 2011.

98. On April 15, 2011, a grand jury indicted the individuals behind www.pokerstars.com alleged bank fraud, money laundering, and illegal gambling offenses. Immediately after the indictment, Western Union transactions from the U.S. to Costa Rica dropped by 50 percent. Western Union employees noted the drop in transactions and associated it with the www.pokerstars.com indictment. As one Western Union employee noted, the pokerstars indictment was a “significant business risk” to Western Union because “[a]bout half of our transaction base appears to have left the system” after the indictment. Compliance employees found the drop in activity “not surprising given the patterns of activity associated with online gaming that we continue to see in Costa Rica.”
99. Western Union employees ultimately found that despite the RTRA program, “Western Union services continue to be used for gaming purposes” between the U.S. and Costa Rica. Throughout 2011 and 2012, Western Union Compliance analysts continued to identify suspicious gambling transactions sent from the U.S. to Costa Rica. Western Union failed to implement a sufficiently effective control against gambling-related transactions.

#### **Western Union’s Remedial Actions and Compliance Enhancements**

100. Since at least September 2012, Western Union took remedial measures and implemented compliance enhancements to improve its anti-fraud and anti-money laundering programs. These remedial measures and compliance enhancements were taken at the direction of the Chief Executive Officer, the General Counsel, and the Chief Compliance Officer and reflect their ongoing commitment to enhancing compliance policies and procedures. These remedial and compliance measures included:
- a. Western Union’s Fraud Risk Management Department—a new Department created in 2012—instituted global Agent oversight standards to identify and investigate any Agent worldwide that processed a certain number of reported fraud transactions.
  - b. Between 2013 and 2015, Western Union increased the number of employees in the Compliance Department by over 100% and increased the Compliance Department budget by over 60%.
  - c. In 2013, Western Union hired a new Chief Compliance Officer and other senior compliance staff. The Chief Compliance Officer has a direct reporting line to the Chairperson of the Compliance Committee of the Western Union Board of Directors.
  - d. Western Union created new compliance procedures to increase compliance authority and accountability, including with regard to Agent oversight. In particular, Western Union created a new AML Oversight Committee, which



meets regularly and has authority to take corrective action against Agents and implement automatic transaction controls such as RTRA rules. Western Union also empowered employees in eight departments to suspend Agents based on analyses, on-site observations, and/or investigation results. Western Union further implemented explicit decision procedures and timelines for Agent oversight actions, including corrective action.

- e. Western Union has continued to increase compliance technology related to Agent oversight. This includes but is not limited to enhancing RTRA rules related to gaming transactions; creating the Agent Complicity Index to identify Agents complicit in fraud; developing new compliance reporting systems to streamline, standardize, and automate certain compliance functions; and enhancing its consumer identification abilities.
- f. Western Union created new teams within its Financial Intelligence Unit to work with law enforcement and generate internal information for Agent and consumer analysis, including a Global Rapid Response Team to reach out to law enforcement proactively with investigative results related to crisis events and Strategic Intelligence Units to identify emerging criminal typologies.
- g. Western Union created and expanded its Courtesy Call Back program, under which certain potentially fraudulent transactions are held while Western Union contacts the sender to determine whether transaction is legitimate.
- h. Western Union expanded fraud reporting mechanisms, including international hotlines, which assist consumers outside the United States in reporting fraud scams to Western Union.
- i. Western Union instituted automatic interdiction of any individual identified in a fraud complaint as the recipient of a fraud-induced transfer and increased interdiction of individuals associated with transactions that exhibited characteristics associated with gambling.
- j. Western Union terminated its relationship with China Corridor Agents that engaged in structuring.
- k. Pursuant to the FTC order, Western Union has taken or will take a number of actions designed to enhance Agent oversight and reduce the risk of fraud.
- l. In addition, pursuant to the FTC Order, Western Union will “reimburse the principal amount of a consumer’s money transfer and any associated transfer fees whenever a consumer or his or her authorized representative reasonably claims that the transfer was fraudulently induced and:
  - i. The consumer or his or her authorized representative asks Defendants, the sending agent, or front line associates to reverse the transfer before the transferred funds have been picked up; or

- ii. Defendants, after reviewing information and data relating to the money transfer, determines that Defendants, their agents or the front line associated failed to comply with any of Defendants’ policies and procedures relating to detecting and preventing fraud-induced money transfers when sending or paying out the money transfer by failing to: provide the required consumer fraud warnings; comply with Defendants’ interdiction or callback programs; verify the recipient’s identification; or accurately record the recipient’s identification(s) and other biographical data.”

ATTACHMENT B

**CERTIFICATE OF CORPORATE RESOLUTIONS**

WHEREAS, THE WESTERN UNION COMPANY (“Western Union” or the “Company”), a financial institution and money services business, has been engaged in discussions with the United States Department of Justice, Criminal Division, Money Laundering and Asset Recovery Section and the United States Attorney’s Offices for the Middle District of Pennsylvania, the Central District of California, the Eastern District of Pennsylvania, and the Southern District of Florida (collectively, the “Offices”) regarding fraud-induced money transfers, money laundering, structuring, gambling-related transfers, and the Company’s anti-money laundering program; and

WHEREAS, in order to resolve such discussions, it is proposed that the Company enter into a deferred prosecution agreement with the Offices (the “Deferred Prosecution Agreement”); and

WHEREAS, the Company’s Executive Vice President and General Counsel, John R. Dye, together with outside counsel for the Company, have advised the Board of Directors of the Company of the Company’s rights, possible defenses, the Sentencing Guidelines’ provisions, and the consequences of entering into such agreement with the Offices;

Therefore, the Board of Directors has RESOLVED that:

1. The Company (a) acknowledges the filing of the two-count Information charging the Company with willfully failing to implement an effective anti-money laundering program, in violation of Title 31, United States Code, Sections 5318(h) and 5322 and regulations issued thereunder, and aiding and abetting wire fraud, in violation of Title 18, United States Code, Sections 1343 and 2; (b) waives indictment on such charges and enters into the Deferred

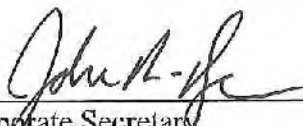
Prosecution Agreement with the Offices; and (c) agrees to forfeit \$ 586 million to the United States;

2. The Company's Executive Vice President and General Counsel, John R. Dye, is hereby authorized, empowered and directed, on behalf of the Company, to execute the Deferred Prosecution Agreement substantially in such form as reviewed by this Board of Directors at this meeting with such changes as the Company's Executive Vice President and General Counsel, John R. Dye, may approve;

3. The Company's Executive Vice President and General Counsel, John R. Dye, is hereby authorized, empowered and directed to take any and all actions as may be necessary or appropriate and to approve the forms, terms or provisions of any agreement or other documents as may be necessary or appropriate, to carry out and effectuate the purpose and intent of the foregoing resolutions; and

4. All of the actions of the Company's Executive Vice President and General Counsel, John R. Dye, which actions would have been authorized by the foregoing resolutions except that such actions were taken prior to the adoption of such resolutions, are hereby severally ratified, confirmed, approved, and adopted as actions on behalf of the Company.

Date: January 18, 2017

By:   
Corporate Secretary  
The Western Union Company

ATTACHMENT C

**ENHANCED COMPLIANCE UNDERTAKING**

In addition to the enhancements the Western Union Company (“Western Union” or the “Company”) has already made to the Company’s anti-fraud and anti-money laundering programs as described in the Statement of Facts, the Company agrees that it has or will undertake the following:

*Board of Directors*

1. The Company has created an independent Compliance Committee of the Board of Directors with direct oversight of the Chief Compliance Officer and the Compliance Program, including anti-money laundering and anti-fraud programs. This Committee is responsible for overseeing the Company’s compliance with all aspects of this Agreement. All reports submitted as a part of this Agreement shall be sent under the cover of this Committee.

*Adopt a Worldwide Compliance and Anti-Money Laundering Standard*

2. As described in Attachment A, the Statement of Facts, “Western Union Agents” or “Agents” are individuals or entities anywhere in the world that own and/or operate businesses that are contractually authorized to offer Western Union’s money transfers to consumers. Western Union Agents include, but are not limited to Independent Agents, Direct Agents, Master Agents, Network Agents or Subagents. The Company has required or will require all Western Union Agents around the world, regardless of their location, to adhere, at a minimum, to U.S. regulatory and anti-money laundering standards, unless in direct conflict with local law.

3. The Company has or will design and implement a risk-based Know Your Agent program to ensure Western Union Agents throughout the world are complying with this policy.
4. The Company has or will create procedures for corrective action, including termination, against Agents—including foreign Agent locations that process transactions to, from, or through the United States—that the Company has determined pose an unacceptable risk of money laundering or the financing of terrorism, or have demonstrated systemic, willful, or repeated lapses in compliance.
5. When the Company identifies Agent locations in violation of law or Western Union policy and procedures, unless asked to do otherwise by law enforcement, or inconsistent with applicable law, the Company will provide notice to the Agent location in writing of the nature of the violation. The Company will require the Agent owner to acknowledge, in writing, that the Agent owner received notice of the violation. The Company will document any training or remedial measures taken by the Company or the Agent owner or location with regard to the violation.

*Executive Review and Bonus Structure*

6. The Company has or will implement evaluation criteria related to compliance in its executive review and bonus system so that each Western Union executive is evaluated on what the executive has done to ensure that the executive's business or department is in compliance with U.S. laws. A failing score in compliance, including anti-money laundering and anti-fraud programs, will make the executive ineligible for any bonus for that year.

7. The Company will include in its new executive review and bonus system a provision that allows the Company to “claw back” bonuses for executives for conduct occurring after the filing of the Agreement that is later determined to have contributed to future compliance failures, subject to applicable law.

*Anti-Fraud Alert System*

8. The Company has or will ensure that all transactions to, from, or through the United States, regardless of the origin or destination, are monitored to identify potentially fraudulent transactions.

*Suspicious Activity Reports*

9. The Company has or will create policies and procedures to ensure that the Company will follow all laws and regulations concerning the filing of Suspicious Activity Reports (“SARs”) in the United States for any suspicious activity, as defined by the Bank Secrecy Act and its implementing regulations. This includes, but is not limited to, filing SARs identifying:
  - a. suspicious activity identified by the Company related to transactions of \$2,000 or more to, from, or through the United States, regardless of where in the world the suspicious transactions originate or are received;
  - b. transactions of \$2,000 or more to, from, or through Agent locations in the United States that are reported by consumers to the Company as fraud-related, regardless of where in the world the suspicious transaction are received;

- c. Agent location owners, operators or employees anywhere in the world that the Company identifies as engaged in or allowing suspicious activity related to transactions of \$2,000 or more to, from, or through the United States.

*High Risk Countries*

10. The Company has or will assign anti-money laundering Compliance Officer(s) to oversee compliance for each country that the Company has designated as high risk for fraud or money laundering. By developing an expertise in their assigned high risk country, the Compliance Officer(s) will better enable the Company to detect and prevent fraud and money laundering activities in those countries.

*Requirements for Reporting*

11. The Company will identify a point of contact within the Company to respond to the Offices' requests.
12. The Company will provide the Offices with reports every ninety (90) days regarding:
  - a. reported consumer fraud complaints, (1) listing all Western Union Agent locations worldwide with ten (10) or more complaints from consumers alleging transactions paid at the Agent location were the result of fraud; (2) for each Agent location on the list, the Company will identify the owner of the Agent location, total fraud complaints for the prior year, total number of receives for the prior year, total dollar value of the receives for the prior year, the average dollar value for receive transactions, total number of sends for the prior year, total dollar value of the sends for the prior year, the average dollar value for send transactions, total revenue earned by Western Union from the Agent location for the prior year



- (including, but not limited to, transfer fees and currency exchange revenue), any additional Agent locations with the same owner, and the total consumer fraud complaints for each other Agent location with the same owner; (3) for each Agent location on the list, the Company will describe what actions, if any, have been taken against the Agent location and/or owner or employees of the Agent location and describe why such action (or lack of action) was deemed appropriate;
- b. SAR reporting, (1) listing all Western Union Agent locations in the United States who are in the top 5% of Agents in terms of SARS filed by the Company; (2) for each Agent location on the list, the Company will identify the owner of the Agent location, total SARS filed by the Company within the reporting period, total SARS filed by the Company for the prior year; and, (3) for each Agent location on the list, the Company will describe what actions, if any, have been taken with regard to the Agent location and/or owner or employees of the Agent location and describe why such action (or lack of action) was deemed appropriate;
- c. corrective action, listing all Western Union Agent locations worldwide that were terminated, suspended or restricted in any way based on fraud, structuring, gambling, or money laundering concerns and whether or not a SAR was filed identifying the Agent location as the subject;
- d. corrective action, listing all Agent location termination, suspension or restriction recommendations by the Company's Fraud Risk Management or Compliance Departments that were not accepted and an explanation of why. The Company

will also indicate whether or not a SAR was filed identifying the Agent location as the subject.

13. The Company will provide the Offices with reports quarterly (1) listing any programs, policies, or procedures designed to detect and prevent illegal gambling-related transactions and (2) summarizing the effectiveness of those programs, policies, or procedures.

*Compliance with the Federal Trade Commission Order*

14. The Company will comply with the FTC Order, including but not limited to, provisions regarding Agent location due diligence; Agent location investigation, suspension, termination, or other disciplinary standards; the Independent Compliance Auditor; consumer fraud reimbursement; and submission of relevant information regarding consumer complaints about alleged fraud-induced money transfers the Company possesses in its fraud database for inclusion in the Consumer Sentinel Network, a secure online database operated by the FTC and available to law enforcement.

*Access to Independent Parties*

15. The Company will provide the Offices with, or will not oppose access by the Offices to, copies of any report, not subject to a valid claim of attorney-client or other privilege, issued by any third party with independent oversight of the Company's anti-money laundering, Bank Secrecy Act, or fraud compliance, appointed as a result of any agreement with U.S. federal or state law enforcement or regulatory agencies. This includes, but is not limited to, the monitor appointed as part of the Company's Agreement with the State of Arizona and the Independent Compliance Auditor appointed as part of

the Company's Agreement with the FTC. The Offices will have direct access to any such third party and may communicate and meet with the third party without the presence of the Company.

**IN THE UNITED STATES DISTRICT COURT  
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA**

_____	)	
FEDERAL TRADE COMMISSION,	)	
	)	
Plaintiff,	)	
	)	Civil Action No.
v.	)	
	)	
THE WESTERN UNION COMPANY,	)	
a corporation, also doing business as	)	
Western Union Financial Services, Inc.,	)	
and through other subsidiaries and affiliates,	)	
	)	
Defendant.	)	
_____	)	

**COMPLAINT FOR PERMANENT INJUNCTIVE  
AND OTHER EQUITABLE RELIEF**

Plaintiff, the Federal Trade Commission (“FTC”), for its complaint alleges:

1. The FTC brings this action under Section 13(b) of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 53(b), and the Telemarketing and Consumer Fraud and Abuse Prevention Act (“Telemarketing Act”), 15 U.S.C. §§ 6101-6108, 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 for Defendant’s acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), and in violation of the FTC’s Trade Regulation Rule entitled “Telemarketing Sales Rule” (“TSR”), 16 C.F.R. Part 310,

in connection with Defendant's failure to take timely, appropriate, and effective measures to mitigate fraud in the processing of money transfers sent by consumers.

### **JURISDICTION AND VENUE**

2. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), and 1345, and 15 U.S.C. §§ 45(a), 53(b), 6102(c), and 6105(b).

3. Venue is proper in this district under 28 U.S.C. § 1391(b)(2), and (c)(2), and 15 U.S.C. § 53(b).

### **PLAINTIFF**

4. The FTC is an independent agency of the United States Government created by statute. 15 U.S.C. §§ 41-58. The FTC enforces 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. The FTC also enforces the Telemarketing Act, 15 U.S.C. §§ 6101-6108. Pursuant to the Telemarketing Act, the FTC promulgated and enforces the TSR, 16 C.F.R. Part 310, which prohibits deceptive and abusive telemarketing acts or practices.

5. The FTC is authorized to initiate federal district court proceedings, by its own attorneys, to enjoin violations of the FTC Act and the TSR, 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), 56(a)(2)(A)-(B), 6102(c), and 6105(b).

**DEFENDANT**

6. Defendant The Western Union Company (“Western Union”), also doing business as Western Union Financial Services, Inc., and through other subsidiaries and affiliates, is a Delaware corporation with its principal place of business at 12500 East Belford Avenue, Englewood, Colorado 80112. Western Union transacts or has transacted business in this district, as well as throughout the United States and the world.

7. Western Union operates, and enters into contracts for the provision of, money transfer services worldwide, through numerous subsidiaries and affiliates, including, but not limited to, Western Union Financial Services, Inc., Western Union Payment Services Ireland Limited (“WUPSIL”), Western Union Payment Services Network EU/EEA Limited, Western Union Financial Services (Canada) Inc., Western Union Network Ireland Ltd., Western Union Network Canada Company, Western Union Network France SAS, Western Union Network Belgium Sprl., Western Union Payment Services UK Ltd., Western Union International Bank GmbH, American Rapid Corporation, Grupo Dinamico Empresarial, S.A. de C.V., Servicio Integral de Envios, S.A. de C.V., and Operaciones Internacionales OV, S.A. DE C.V.

## **COMMERCE**

8. At all times material to this Complaint, Defendant has 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.

## **BACKGROUND**

9. For many years, Western Union’s money transfer system has been used by fraudsters around the world to obtain money from their victims. Discrete subsets of Western Union agents in various countries have largely been responsible for processing the payments, and many Western Union agents have played active and important roles in facilitating those frauds. As described more fully below, although Western Union has long been aware and has received many warnings that its system is being used for frauds, for many years it has failed to implement adequate and effective policies and procedures to detect and prevent fraud and to take prompt action to effectively address problematic agent locations. In some instances, Western Union’s agent locations have been, or likely been, complicit in the frauds, and have engaged in suspicious activities indicative of complicity in paying out fraud-induced money transfers. In other cases, Western Union’s agent locations have facilitated the scams by paying out fraud-induced money transfers in violation of Western Union’s anti-fraud and/or Anti-Money Laundering (“AML”) policies and procedures that impact consumer fraud. Western Union has

known about the problem and has identified many of the agents providing substantial assistance or support to the frauds. Although as a result of the FTC's investigation, Western Union has improved aspects of its anti-fraud program since 2012, Western Union still has failed in many cases to promptly suspend and terminate agent locations facilitating fraud. Instead, Western Union has continued to profit from the activities of these agents.

### **Western Union's Money Transfer System**

10. Western Union offers money transfer services to consumers worldwide through a network of approximately 515,000 agent locations in more than 200 countries and territories. Western Union is the largest money transfer company in the United States and worldwide. More than 50,000 of its 515,000 agent locations are in the United States. In addition to offering money transfer services under the Western Union brand, Western Union owns and operates Orlanda Valuta ("OV"), which provides money transfer services primarily to Mexico, and Vigo, which provides money transfer services primarily to Latin America and the Caribbean. Consumers in the United States can send money transfers through OV and Vigo from thousands of Western Union agent locations. According to Western Union, "[e]very day, millions of consumers rely on Western Union Money Transfer® service to send money to loved ones near and far."



11. Consumers wishing to send funds using Western Union's money transfer system may initiate a transaction in person, online, or over the telephone. Western Union claims that its locations are "around every corner" with "knowledgeable agents," and that its money transfer services are "fast, convenient, and safe." Although the amount that may be sent online or over the telephone is sometimes restricted, there typically are no restrictions on the amount of money that a consumer can send in person from agent locations. Certain countries, however, limit the amount of money that can be picked up from agent locations. For in-person money transfers, consumers must pay with cash or a bank-issued debit card. For online or telephone transfers, consumers typically must pay with a credit or debit card. Over 90% of money transfers sent through Western Union are initiated in person at Western Union's agent locations.

12. When initiating a money transfer at one of Western Union's agent locations, the sender must complete a "send form," which typically requires the sender's name, address and telephone number, and the name of the recipient and the city, state/province, and country to which the money transfer is being sent. Consumers initiating money transfers at Western Union's agent locations may select from Western Union's "Money in Minutes" or "Next Day" services, where available. For money transfers above a certain amount, such as \$1,000, the sender must present identification ("ID") and the agent locations must record in Western

Union's system the sender's ID information. Over time, in some countries, Western Union has lowered the amount that triggers the ID requirement.

13. In order to send a money transfer, consumers must pay a fee to Western Union. This fee varies depending upon the method of the money transfer, the destination, the amount, the method of payment, and how quickly the money transfer is to be completed. The money transfer fee for Western Union's "Money in Minutes" service is higher than its "Next Day" service. According to Western Union's website, to send a \$1,000 "Money in Minutes" money transfer from the United States to the United Kingdom ("UK"), consumers must pay an \$81 transfer fee if paying by credit or debit card, or \$58 if paying in cash. For international money transfers, in addition to charging consumers a money transfer fee, Western Union also makes money from the foreign currency exchange. Upon initiating a money transfer, consumers are provided with a unique tracking number called a Money Transfer Control Number ("MTCN").

14. Prior to paying out funds at its agent locations, Western Union's practice is generally to require the recipient to provide the MTCN, to complete a "receive form" with the recipient's name, address and telephone number, and to present ID. For many years, for money transfers of less than \$1,000, even though recipients may have been required to present ID, Western Union agent locations worldwide have not been required to record in Western Union's system the

recipient's ID information. When the recipient does not have an ID and the money transfer is less than \$1,000, the sender sometimes has the option of using a "Test Question and Answer." According to Western Union, this option "is designed for emergency situations where the receiver doesn't have proper identification" because his or her wallet was stolen.

15. Regardless of the method used to initiate the money transfer, all Western Union money transfers flow through the same global money transfer system controlled by Western Union. This system coordinates and makes funds available to complete the transactions. Agents must have active accounts with Western Union to send and receive money transfers using Western Union's money transfer system.

16. Once Western Union's agent locations have paid out the funds, Western Union's policy typically is that the sender cannot obtain a refund from Western Union of either the amount transferred or the money transfer fee, even if the sender was a victim of fraud or the money transfer was paid out to someone other than the intended recipient. The policy even applies if the Western Union agent location was complicit in the fraud, engaged in suspicious activity, or failed to follow Western Union's policies and procedures when processing the money transfer (*e.g.*, by failing to record the recipient's ID or other required information).

### **Use of Western Union's Money Transfer System to Facilitate Fraud and Harm Consumers**

17. Over the years, money transfers have increasingly become the payment method of choice for scams that prey on consumers around the world. Fraudulent telemarketers and con artists prefer to use money transfers to facilitate their scams because, among other reasons, they can pick up money transferred within minutes at multiple locations and, oftentimes, the perpetrators are afforded anonymity because the payments are untraceable. For example, money transfers can be picked up at any location within a particular state or country; some money transfers can be picked up without presenting or having to record an ID; fake names, addresses, and IDs sometimes can be used; and Western Union's own agent locations sometimes fail to follow the company's policies and procedures in paying out money transfers, and in other instances, are complicit in the frauds. Therefore, it is often difficult for consumers and law enforcement to identify and locate the recipients of fraud-induced money transfers.

18. Western Union maintains a database of complaints it receives about fraud-induced money transfers. Based on information in that database, between January 1, 2004 and August 29, 2015, Western Union received at least 550,928 complaints about fraud-induced money transfers, totaling at least \$632,721,044. Over 80% of the complaints in the database were from U.S. consumers. The average individual consumer fraud loss reflected in that database was

approximately \$1,148. That is more than three times the amount of Western Union's average money transfer for the years 2010 through 2014—approximately \$346—and more than seven times the amount of Western Union's median money transfer for the same period—approximately \$162.

19. As explained more fully below, the complaints in Western Union's database represent only a small percentage of the actual fraud perpetrated through Western Union's money transfer system because most victimized consumers do not complain directly to Western Union. In addition, Western Union also does not include information in its database about all of the complaints it receives. Therefore, since at least January 1, 2004, it is likely that Western Union's money transfer system has been used to send billions of dollars in fraud-induced payments to telemarketers and con artists worldwide.

**Western Union's Contractual Authority  
to Oversee and Take Action Against its Agents**

20. Western Union requires that its agents, which are also referred to as authorized delegates or representatives, sign written agreements in order to offer and provide payment services through Western Union's money transfer system. The initial terms of the written agreements typically are five years, after which they are renewable for additional periods of time. Western Union pays its agents in the United States an agreed-upon commission, performance bonus, and volume bonus for offering and processing money transfer services on Western Union's

behalf, while it pays its international agents an agreed-upon base compensation for the consumer fee received, and a percentage of the foreign exchange profits, on each transaction.

21. Western Union's written agreements with its agents typically require the agents to comply with all applicable laws, including laws for detecting and preventing money laundering. These agreements also provide that Western Union has the right to immediately suspend or terminate its agents, including any agent location. Western Union's agents are required to keep records for all transactions, provide them to Western Union upon request, and cooperate with any audit or review by Western Union. The agreements also provide Western Union with the right to inspect and audit its agents' books and records to monitor the agents' compliance with the agreement, applicable law, and Western Union's policies.

22. Western Union's agents, which are also sometimes referred to as "network agents," "master agents," or "super-agents," in many instances provide Western Union's money transfer services through their own networks or locations, or, in countries outside of the United States and Canada, also through sub-representatives, which Western Union commonly refers to as "subagents" (hereinafter collectively referred to as "agents" or "subagents"). Western Union typically is not involved in enrolling its agents' subagents and does not have a direct contractual relationship with them. Western Union's agreements with its

agents, however, provide it with the authority to suspend and terminate its agents' subagents, as well as any location at which its money transfer services are offered.

### **Western Union's Programs, Policies, and Procedures**

23. Western Union has two primary programs relating to the detection and prevention of consumer fraud and the installation and oversight of agents: its anti-fraud program, which sometimes is referred to as its consumer protection program, and its AML program. As implemented by Western Union, for many years these interrelated programs failed to adequately and effectively detect and prevent consumer frauds employing Western Union's money transfer system. Western Union's design and implementation of these programs for addressing fraud, as well as its oversight of its global money transfer system, occur primarily within the United States.

24. For many years, Western Union has failed to implement a comprehensive and effective anti-fraud program. In or around April 2003, after Western Union became aware that some of its agents had been suspected of being involved in paying out fraud-induced money transfers to telemarketers, Western Union's Security Department developed a Standard Operating Procedure ("SOP") for reviewing and suspending agents for consumer fraud. The SOP outlines a process and guidelines for identifying agents for review and suspension based on consumer fraud complaints, as well as a process for reinstating or terminating

agents. The SOP was revised at various times, most recently in or around September 2010. Beginning in or around January 2006, the SOP included procedures that applied to agents outside of the United States and Canada. However, to the extent that Western Union suspended and/or terminated agents pursuant to the SOP, for many years the suspensions and/or terminations were typically limited to agents in the United States and Canada.

25. In a written report in January 2011, Western Union represented it was making “enhancements” to its consumer protection program that were to include improvements to the company’s program for conducting due diligence and training of its agents, monitoring agent activity, and taking disciplinary action, including suspension and termination, against agents. Subsequently, in a written report about its anti-fraud program dated September 14, 2012, Western Union claimed it had implemented “a comprehensive anti-fraud program” that included agent training, agent monitoring, and “[p]rompt action, including suspensions and terminations, against Agents when the Company identifies fraudulent activity.” Western Union recognized in this report that its “first line of defense against fraud is to engage Agents who will fully comply with the Anti-Fraud program and policies and procedures.”

26. As a result of the FTC’s investigation, Western Union has made progress since 2012 in identifying and blocking potentially fraudulent transactions



and in otherwise protecting consumers from fraud. Despite that, Western Union continued to fail, in certain cases, to promptly suspend and terminate certain high-fraud agent locations, including locations that appeared to be complicit in paying out fraud-induced money transfers or repeatedly failed to comply with Western Union's anti-fraud and AML programs, policies, and procedures.

27. In addition to its anti-fraud program, Western Union is required by the Bank Secrecy Act ("BSA") to have an effective AML program to guard against money laundering, including, but not limited to, guarding against the flow of illicit funds, such as funds derived from fraud. As part of its AML program, Western Union has developed Know Your Agent guidelines and policies, and policies and procedures for monitoring transaction, customer, and agent activity for risks, including suspicious activity and agent complicity. Western Union's AML program relies heavily upon its agents to have their own AML programs. In many cases, Western Union or its agents have failed to implement effective AML policies and procedures pertaining to consumer fraud, thereby making Western Union's money transfer system more vulnerable to consumer fraud.

28. As described below, Western Union has failed to: promptly investigate, suspend, and terminate potentially complicit agents and subagents, or agents and subagents that have failed to comply with Western Union's anti-fraud and/or AML policies and procedures that impact consumer fraud; conduct

adequate due diligence on prospective and existing agents and subagents; effectively train, monitor, and review agents, subagents, and front line associates, who are responsible at the point of sale for processing money transfers at Western Union's agent locations ("FLAs"), with respect to consumer fraud; adequately collect, record, and report consumer fraud involving its money transfer system; and adopt other reasonable measures to prevent fraud-induced money transfers. In some cases Western Union has failed to adopt adequate and effective policies and procedures to detect and prevent fraud-induced money transfers, while in other cases it has failed to adhere to its own anti-fraud and AML programs, policies, and procedures.

**WESTERN UNION'S MONEY TRANSFER  
SYSTEM HAS REGULARLY BEEN USED FOR FRAUD**

29. Perpetrators of many different types of mass marketing and imposter scams have relied on money transfer systems, including Western Union's system, as a means of fraudulently obtaining money from consumers around the world. All of these scams operate deceptively in violation of Section 5 of the FTC Act, and many of the scams also involve fraudulent telemarketing in violation of the TSR.

30. In these scams, consumers often are instructed over the telephone or by email to send money transfers through Western Union's money transfer system. The telemarketers and con artists use false or misleading statements to induce consumers either to pay for purported goods or services, or to make payments as a

result of purported circumstances, such as emergencies, that do not exist.

Consumers' fraud-induced payments through Western Union's system often exceed \$1,000 per transaction. The types of scams referenced in Western Union's own complaint database include, but are not limited to:

- a. *Online or Internet purchases* (see FTC Consumer Alert on Online purchases, available at <http://www.ftc.gov/news-events/press-releases/2006/07/ftc-advises-consumers-not-use-wire-transfers-online-purchases>): According to Western Union's complaint database, between January 1, 2004 and August 29, 2015, the company received at least 146,909 complaints about this type of scam totaling at least \$187,877,003 in losses;
- b. *Lottery or prize scams* (see <http://www.consumer.ftc.gov/articles/0086-international-lottery-scams>): According to Western Union's complaint database, between January 1, 2004 and August 29, 2015, the company received at least 75,543 complaints about this type of scam totaling at least \$86,138,055 in losses;
- c. *Emergency scams, including grandparent scams* (see <http://www.consumer.ftc.gov/articles/0204-family-emergency-scams>): According to Western Union's complaint database, between January

1, 2004 and August 29, 2015, the company received at least 41,897 complaints about this type of scam totaling at least \$73,807,353 in losses;

d. *Advance-fee loan scams* (see

<http://www.consumer.ftc.gov/articles/0078-advance-fee-loans>):

According to Western Union's complaint database, between January 1, 2004 and August 29, 2015, the company received at least 71,296 complaints about this type of scam totaling at least \$43,617,107 in losses; and

e. *Online dating or romance scams* (see [http://www.ftc.gov/news-](http://www.ftc.gov/news-events/press-releases/2010/11/ftc-warns-consumers-about-online-dating-scams)

[events/press-releases/2010/11/ftc-warns-consumers-about-online-](http://www.ftc.gov/news-events/press-releases/2010/11/ftc-warns-consumers-about-online-dating-scams)

[dating-scams](http://www.ftc.gov/news-events/press-releases/2010/11/ftc-warns-consumers-about-online-dating-scams)): According to Western Union's complaint database,

between January 1, 2004 and August 29, 2015, the company received at least 44,588 complaints about this type of scam totaling at least \$40,980,482 in losses.

31. When consumers send the money transfers from one of Western Union's agent locations, the perpetrators of the scams described above, or those acting on their behalf, frequently collect the funds from one of Western Union's corrupt or complicit agent locations or from agent locations that violate Western Union's anti-fraud and/or AML policies and procedures, such as by failing to

properly collect and record all of recipients' IDs or biological information, or by recording obviously false information.

**A DISCRETE SUBSET OF WESTERN UNION  
AGENTS WORLDWIDE HAS PAID OUT THE  
MAJORITY OF FRAUD-INDUCED MONEY TRANSFERS**

32. Western Union's records show that the majority of fraud-induced money transfers have been paid out by a discrete, and easily identifiable, subset of Western Union's agents and subagents in various countries around the world. The vast majority of Western Union agent locations worldwide do not pay out transactions associated with a single fraud complaint to Western Union. In fact, only a small and discrete subset of agents and subagents worldwide pay out money transfers relating to any fraud complaints. An even more easily identifiable and distinct subset of agents and subagents have been the subject of five or more fraud complaints in a given year, but this group of Western Union agents has been responsible for paying out most of the reported fraud losses. For example:

- a. In 2012, 137 agent locations in Mexico (out of an average of 17,710 locations operating in that country each month of the year) had five or more fraud complaints, and these 137 agents were responsible for paying out approximately \$3.2 million, amounting to over 80% of the total reported fraud for Mexico that year. Similarly, in 2013, 140 agent locations in Mexico (out of an average of 9,002 locations) paid

out approximately \$2.1 million, amounting to over 75% of the total reported fraud in Mexico, and in 2014, 108 agent locations (out of an average of 8,345 locations) paid out approximately \$1.5 million, amounting to over 76% of the total reported fraud.

b. In 2012, 188 agent locations in Nigeria (out of an average of 5,036 locations in that country) had five or more fraud complaints, and these 188 agents paid out approximately \$1.9 million, amounting to over 77% of the total reported fraud for Nigeria that year. In 2013, 235 agent locations in Nigeria (out of an average of 5,034 locations) paid out approximately \$1.5 million, amounting to over 71% of the total reported fraud in Nigeria, and in 2014, 269 agent locations (out of an average of 5,208 locations) paid out approximately \$2.6 million, amounting to over 84% of the total reported fraud.

33. Western Union’s internal reports and memoranda show that the company was aware that discrete and easily identifiable subsets of agents and subagents in various locations were responsible for paying out the majority of fraud-induced money transfers. For example, a Financial Intelligence Report titled “G.A.P. – United Kingdom” stated that a review of fraud complaints in late 2009 revealed that one network of agents “accounted for more consumer Fraud Complaints than any other Agent Network in the United Kingdom” and that an

analysis of data in the first quarter of 2010 for nineteen agents demonstrated “indicators of Agent complicity.” A January 19, 2012 memorandum regarding “GMI Fraud Monitoring and Intelligence” stated that in Spain “when looking at a list of 30 Agents that were investigated in 2010 it was determined that the amount of potential fraud identified by GMI surpassed the *total number of formal fraud complaints and amounts for the entire country in 2010*, demonstrating the true levels of fraud related risk present in Spain.” (Emphasis in original.) In March 2012, a senior compliance analyst found that from December 1, 2011 to February 24, 2012, “nearly 85% of all emergency fund fraud complaints filed with Western Union” involved money transfers paid out by one master agent in Mexico, Elektra, through 94 of its locations.

**MANY WESTERN UNION AGENTS HAVE BEEN  
ACTIVE OR COMPLICIT IN THE UNDERLYING SCAMS**

34. Many Western Union agent locations that have received fraud-induced money transfers from consumers and paid out such transfers to the fraudulent telemarketers and con artists have been complicit in the underlying scams. In some cases, the sellers, telemarketers, or imposters who have operated the scams have been Western Union’s own agents or subagents.

35. At least 146 of Western Union’s agents and subagents around the world, as well as at least two FLAs, have been charged with acting collusively in the frauds employing Western Union’s money transfer system. Of the 146 agents,

39 agents in the United States and Canada have been charged in the United States with defrauding consumers through various mass marketing and/or telemarketing schemes including fraudulent sweepstakes, advance fee loans, business opportunities (including secret shopper or work-at-home scams), emergency or person-in-need schemes, and/or Internet purchase offers. The charges against these 39 agents have included conspiracy to commit mail fraud, wire fraud and/or money laundering, and most of the agents have already pleaded guilty or been convicted of the charges. These 39 agents paid out over \$5.2 million in money transfers that were reported to Western Union as having been induced by fraud. As explained below, however, actual consumer losses far exceed the reported losses.

These matters include:

<b>Case</b>	<b>Western Union Agents</b>
<i>United States v. Agbasi, et al.</i> , No. 07-CR-504 (M.D. Pa.)	Stanley Akubueze and Christopher Ozurus (d/b/a Afro Spot Restaurant) Philip Utomi (d/b/a Swift Cash Centre)
<i>United States v. Bellini, et al.</i> , No. 07-CR-1402 (C.D. Cal.)	Vijayakumar Ramakrishnan (d/b/a Cafe Chambly) John Felix Alexander (d/b/a Imudia Int)
<i>United States v. Ayodele, et al.</i> , No. 10-CR-058 (M.D. Pa.)	Soji Ayodele (d/b/a Total Communications Centre) Mohsen Golab (d/b/a Golden Century) Christian Kevin (d/b/a C K Business Service)
<i>United States v. Akinola, et al.</i> , No. 10-CR-300 (S.D. Tex.)	Jonathan Akinola (d/b/a Postal & Wireless Outlet)
<i>United States v. Groysman</i> , No. 10-CR-326 (M.D. Pa.)	Bella Groysman (d/b/a Professional Medical Supplies)



<i>United States v. Dobrovinsky-Kaz</i> , No. 10-CR-327 (M.D. Pa.)	Tatyana Dobrovinsky-Kaz (d/b/a Professional Medical Supplies)
<i>United States v. Abbey</i> , No. 10-CR-344 (M.D. Pa.)	Festus G. Abbey (d/b/a Abbey's One Stop and Abbey Multi Service)
<i>United States v. Nwuda</i> , No. 10-CR-508 (C.D. Cal.)	Nmandi Nick Nwuda (d/b/a CKane Check Cashing & Postal)
<i>United States v. Idemudia</i> , No. 11-CR-001 (M.D. Pa.)	Eugene Idemudia (d/b/a IV Beauty Supply and RM & E)
<i>United States v. Agho, et al.</i> , No. 11-CR-113 (M.D. Pa.)	Betty Agho (d/b/a Star Multiservice) Itohan Agho-Allen (d/b/a Miracle Multi Link) Prince Edosa (d/b/a Gosa Multi Services and A & M Communications) Kennedy Onaiwu (d/b/a Kenizo Enterprise) Ikejiani Okoloubu (d/b/a First Cone and Depanneur Ice) Susan Osagiede (d/b/a A & M Communications) Elvis Uadie (d/b/a Diale Investment) Nekpen Omorodion (d/b/a Global Multiservices)
<i>United States v. Adigun, et al.</i> , No. 11-CR-151 (M.D. Pa.)	Olufemi Adigun (d/b/a FAB)
<i>United States v. Louissaint</i> , No. 11-CR-201 (M.D. Pa.)	Emmanuel Louissaint (d/b/a Hudson Food Market II)
<i>United States v. Brown</i> , No. 12-CR-001 (M.D. Pa.)	Blessing Brown (d/b/a O & B Enterprise Inc)
<i>United States v. Mayele</i> , No. 12-CR-210 (C.D. Cal.)	Prince Martin Mayele (d/b/a Du Monde Digital Trades)
<i>United States v. Mgbolu, et al.</i> , No. 12-CR-232 (M.D. Pa.)	Alex Mgbolu (d/b/a FA CAM Assoc. & Financial Corp) Chima Nneji (d/b/a Advanced Computer Service and Hallmark Business Services) William Nneji (d/b/a Hallmark Business Services)

<i>United States v. Idisi-Arah, et al.</i> , No. 12-CR-311 (M.D. Pa.)	Lucas Obi (d/b/a Canada Cash Express)
<i>United States v. Anyika, et al.</i> , No. 14-CR-006 (M.D. Pa.)	Ejike Egwuekwe (d/b/a Merrick Multiple Services and Lincoln One Stop Place) Franklyn Idehen (d/b/a Treasure Links and Cherrish Communication Center) Nnamdi Ihezuo (d/b/a Net Global & Multi Services) Cyprian Osita Ngbadi (d/b/a Rockaway Business Center)
<i>State of Texas v. Mbaka</i> , No. 09-DCR-52310A (Tex. Dist. Ct. Ft. Bend County)	Boniface Ifeanyi Mbaka (d/b/a BIM Services)

36. Criminal law enforcers in other countries also have taken action against at least an additional 107 Western Union agents and two FLAs, including in the following instances:

- a. Sentencing in the UK (in or around November 2012) of an individual, Peter Oyewor, who operated at least two Western Union agent locations (d/b/a Benson Logistics and Abmec Logistic) and was found guilty of money laundering over £1.34 million in proceeds from consumer frauds;
- b. Arrests made by the Nigerian Special Fraud Unit (in or around June 2013) of two FLAs at a Western Union location (Skye Bank PLC) for aiding Internet fraudsters; and
- c. Arrests made by the Spanish police (in or around July 2014) of 105 Western Union agents in Spain, who were involved in a massive

international scam involving Nigerian frauds that primarily targeted U.S., Canadian, and German consumers, and caused at least €11.5 million (approximately \$15.5 million) in consumer injury.

**WESTERN UNION HAS BEEN AWARE THAT ITS SYSTEM HAS BEEN USED FOR FRAUD-INDUCED MONEY TRANSFERS**

37. Since at least January 2004, Western Union has been aware that its system has regularly been used for fraud and that it has an identifiable subset of agents and subagents with high levels of fraud complaints. It also has been aware that many of its agent locations with high-fraud payouts have: (1) violated Western Union's anti-fraud and/or AML policies and procedures; (2) engaged in suspicious activities; and/or (3) been complicit, or likely complicit, in the frauds. Western Union's awareness of the consumer fraud problem is demonstrated by, among other things, the hundreds of thousands of complaints it has received from consumers, its own internal records and reports, and years of warnings from government agencies throughout the world.

**Defrauded Consumers Have Regularly Complained to Western Union**

38. When consumers realize that they have been defrauded, they sometimes contact Western Union to report the fraud, often using a toll-free number made available by Western Union to consumers in certain countries, including the United States. In some cases, consumers also have filed lawsuits against Western Union due to the company's role in processing the fraud-induced

money transfers. In addition, as described above, between approximately January 1, 2004 and August 29, 2015, Western Union's database shows at least 550,928 complaints it received about at least \$632,721,044 in fraud-induced money transfers. Western Union also has other records reflecting additional complaints it received, which were not recorded in the database, including a spreadsheet of at least 8,497 complaints Western Union received in 2005 regarding fraud-induced money transfers, which totaled at least \$14,478,365.

39. The complaints reported to Western Union, however, represent only a fraction of the consumer frauds employing Western Union's money transfer system for at least three reasons:

- a. For years, Western Union has failed to provide victims in many countries worldwide with access to a fraud hotline, or a toll-free telephone number for victims to call to report fraud, which is the most convenient mechanism for many victims to promptly report fraud;
- b. The majority of consumer victims do not complain directly to Western Union. Western Union's own internal reports recognize that only a small percentage of consumers complain about fraud and that the volume of fraud-induced money transfers is much higher than that reported to the company. For example, Western Union has recognized in several reports that the actual amount of fraud-induced

money transfers associated with agent locations was in some cases over five times higher than the reported complaint figures; and

c. As further explained below, Western Union's database of fraud complaints is incomplete because Western Union has failed to log in its database all of the complaints and reports about fraud it has received, as well as all of the fraud-induced money transfers related to the complaints.

**Western Union's Internal Reports and Records Demonstrate Awareness of Consumer Fraud by Agents in Various Countries Worldwide**

40. Since at least 2005, Western Union has conducted reviews and investigations, and generated indices and reports, related to consumer fraud involving its money transfer system. Information contained in Western Union's internal reports, communications, and other records demonstrates that the company has been aware of high levels of consumer fraud involving particular countries and agents, including network agents Western Union itself owns. These records demonstrate serious problems and suspicious activities by particular Western Union agents and subagents, including, but not limited to: (a) high numbers and patterns of complaints; (b) spikes in the number of money transfers received; (c) money transfer amounts that far exceed the average transfer amount; (d) data integrity issues (issues relating to the recording of ID numbers, dates of birth, or other information about recipients); (e) payouts within minutes after the money

transfers were sent; (f) flipping (shortly after receiving funds, a large portion of the money is sent to another recipient); (g) surfing (suspicious look-ups of money transfers in Western Union's system by FLAs); and (h) substantial sends to high-risk countries known for fraud.

41. According to information contained in Western Union's complaint database, the United States has been the top country for fraud payouts since at least 2004 and has generated over three times the number of complaints as the next highest country. In fact, over \$128.2 million in reported fraud has been paid out in the United States since 2010, and Western Union has received more than 34,000 fraud complaints about transactions totaling over \$21.2 million since 2014. Certain agent locations in the United States have operated for years despite high levels of fraud. For example, between July 2008 and March 2015, one agent location in Washington, D.C. generated at least 116 fraud complaints totaling \$187,356. Even though reviews of the agent in June 2014 and February 2015 identified confirmed and potential fraud amounting to 84% and 55% of the money transfers paid at that location, the agent was not terminated until August 2015, after it failed an undercover test visit by a compliance officer tasked with assessing the agent's AML compliance. Another agent location in Detroit, Michigan, paid out at least 194 money transfers totaling \$379,031 in reported fraud since 2004.

Although this agent has received Western Union's fraud prevention training multiple times, it has continued to receive fraud complaints.

42. Over the years, many other countries in addition to the United States have emerged as high-risk countries for fraud as international scams have become more pervasive. For example, from 2006 to 2012, the UK was the second highest-payout country for fraud-induced money transfers behind the United States. During that time, Western Union's UK agents paid out over \$82.4 million in reported fraud, and internal reports and records demonstrate that Western Union was aware of problems with particular agents in the UK. From January 1, 2004 to August 29, 2015, 172 UK agents paid out over \$44.3 million in reported fraud. A subset of only 34 of these agents was responsible for paying out nearly half of the reported fraud (at least \$21.2 million), most of which came from U.S. victims. The actual fraud paid out by these agents was likely much higher. Total payouts by these agents during the period they were receiving fraud complaints amounted to \$389 million, with \$154 million of that coming from U.S. senders. Notably, these agents also sent \$104.6 million to Nigeria and \$76.6 million to Romania, both of which are high-risk countries for fraud, as acknowledged by Western Union itself. One agent alone, News Mark, was the top fraud agent in the UK and worldwide. Between January 1, 2006 and January 14, 2013, Western Union received at least 1,421 fraud complaints about News Mark totaling at least \$2,150,892, of which

over 84%, or \$1,815,582, involved U.S. victims. Although Western Union identified News Mark as a high-fraud agent in the company's 60-day reports at least 45 times between 2005 and 2010, and reviewed it for fraud and other suspicious activities at least fifteen times between 2009 and 2012, Western Union suspended and reactivated News Mark at least three different times before finally terminating it in 2014.

43. By 2007, Western Union was aware that Jamaica had become a hotbed for fraud. In that year alone, Western Union received at least 3,065 complaints from U.S. consumers about money transfers totaling \$1,878,435 to Jamaica. Over the years, the top four fraud payout agents in Jamaica have processed well over \$1 million each in reported fraud, for a combined total of at least \$5,210,644. According to internal Western Union reports, those agents also have engaged in other highly suspicious activities, such as surfing. One of those agents, for example, surfed at least 985 transactions in a single month in 2010. Even though all four of these agents have continued to receive many fraud complaints for years, including hundreds in 2015, they continue to operate. In fact, Western Union has only terminated one agent in Jamaica for consumer fraud. That termination occurred on July 3, 2015, and the terminated agent had a much smaller number of fraud complaints than others that Western Union has not terminated.



44. In 2008, according to Western Union's records, Mexico was one of the top five countries worldwide for fraud payouts, with 1,393 complaints totaling over \$1.8 million. In 2009, Mexico was Western Union's sixth highest payout destination, with 1,626 complaints totaling over \$2.1 million. Since 2011, it has consistently been in the top three destination countries for reported fraud payouts from U.S. consumers, and the top payout destination for fraud related to emergency scams. In 2011, Western Union received at least 2,824 emergency scam complaints on transfers paid out in Mexico. The total amount paid out on these transfers was \$6,908,666, and the average payout was \$2,446. Of those victims who reported their date of birth, nearly 70% were 65 years or older at the time they sent their money transfers. Although Western Union has at least three master agents in Mexico, internal reports and records show that one master agent, Elektra, has been responsible for paying out most of the emergency scam complaints. Of the reported emergency scam transfers paid out in Mexico between 2011 and 2014, Elektra agents were responsible for payouts relating to at least 7,107 complaints totaling \$12,494,602, or 88% of the total reported losses. During that same period, nineteen Elektra agents paid out \$6,425,782 in reported emergency fraud, including one agent discussed further below that alone paid out over \$1.4 million in reported fraud. Nevertheless, and despite repeated reviews and investigations of agent locations in Mexico, as of October 2015, Western

Union had rarely, if ever, terminated agent locations in Mexico for consumer fraud, even in instances where particular agent locations repeatedly appeared on fraud reports, or had confirmed and potential fraud amounting to more than 25%, or even 50%, of their payouts.

45. By 2010, internal reports and records show that Western Union was aware of a substantial increase in fraud complaints involving money transfers sent to Spain, and that particular agents there had very high levels of fraud and questionable activity. From 2009 to 2010, the number of complaints paid out in Spain increased from 583 to 2,195, and the reported fraud amount rose from over \$1.1 million to over \$5.3 million. Indeed, from 2010 to 2012, Spain was the third highest payout country by amount for complained-of transfers, trailing only the United States and the UK. During that time, Western Union received at least 8,086 complaints about transfers paid out in Spain, totaling over \$17 million. From 2007 to 2012, a subset of 61 agents in Spain paid out over \$11.9 million in reported fraud. Western Union's internal reports and records document numerous instances of suspicious activity by these agents, including flipping and sending money transfers to high-risk countries. The reported fraud paid out by agents in Spain, moreover, likely grossly understates the actual fraud. For example, 20 agents in Spain that were responsible for over \$5.7 million in reported fraud received more than \$51.6 million during the period those agents were receiving fraud complaints,

of which over \$22.7 million came from U.S. consumers. During that time, those 20 agents were responsible for sending over \$8.8 million to Nigeria, over \$3.7 million to Canada, over \$1.7 million to Romania, and over \$800,000 to Ghana, which are all high-risk fraud countries. Although Western Union was aware of problematic agent locations in Spain, it failed to promptly suspend and terminate those agent locations.

46. Prior to 2011, Western Union received a small number of complaints each year involving its Peruvian agents. For example, in 2010, Western Union recorded only 71 fraud reports against agents in Peru totaling \$38,492. In 2011, however, there was a dramatic spike in complaints about money transfers paid out in Peru, especially about emergency scams, with Western Union receiving at least 692 complaints totaling \$2,218,761. The average transfer amount in the complained-of transactions jumped from \$542 to \$3,206. In 2012, the numbers increased to 1,003 fraud complaints totaling \$1,944,730. Over 96% of the complained-of transfers paid out in Peru in 2011 and 2012 originated from the United States. Between 2011 and 2012, thirteen Peruvian agents paid out \$3,603,539 in reported fraud, and together were responsible for nearly 87% of the total reported fraud payouts in Peru for those years. Internal reports and records show that Western Union was aware of the dramatic increase in complaints, as well as particular Peruvian agent locations that were responsible for paying out

most of the reported fraud. Despite its awareness, Western Union failed to terminate problematic agent locations until after law enforcement began to inquire and raise concerns about the fraud, and even then, one agent location terminated for consumer fraud was reactivated under a different agent ID. In recent years, Western Union has continued to receive complaints from U.S. consumers concerning high-dollar emergency scam-related money transfers paid out at agent locations in Peru.

47. For many years, Nigerian scammers have been at the center of many international frauds. Although Western Union's agent locations in Nigeria are in banks, those bank locations, too, have paid out large numbers of fraud-induced money transfers and engaged in other suspicious activities. According to Western Union's records, Nigeria has been the fourth highest payout destination for fraud complaints received by Western Union since 2006. Since then, Western Union has received complaints about at least 48,047 money transfers paid out in Nigeria, totaling over \$38.2 million. Approximately 86.7% of the complained-of transfers originated from the United States. During this period, a subset of 68 Western Union agent locations in Nigeria was responsible for at least 17,743 complaints totaling over \$16.6 million in reported fraud. Based on the complaints, reported fraud is typically paid out at various locations of two large banks in Nigeria. Overall, one of those banks has at least 15,184 complaints totaling \$11,292,195,

while the other has at least 10,948 complaints totaling \$8,167,769. Individual locations of the two banks also have amassed huge numbers of complaints. One location alone was responsible for at least 832 complaints totaling \$1,407,252, while another was responsible for at least 1,741 complaints totaling \$1,187,141. Despite repeated reviews and investigations of agent locations in Nigeria, as of October 2015, Western Union had rarely, if ever, terminated agent locations in Nigeria for consumer fraud.

48. Over the years, agent locations in many other countries have appeared on Western Union's fraud reports, and have been reviewed by the company for fraud. Those countries include, but are not limited to, Ghana, the Philippines, Bolivia, China, Malaysia, the Dominican Republic, Greece, and Thailand. Some of those agent locations continue to operate despite having high levels of fraud, while others have been suspended or terminated, but only after having caused substantial injury to consumers over many months or, in some cases, years.

**Government Agencies Worldwide Warned  
Western Union about Consumer Fraud Involving Its System**

49. In addition to consumer complaints and Western Union's internal reports and records, Western Union's awareness of the consumer fraud problem with its money transfer system is further demonstrated by the fact that law enforcement agencies in the United States and throughout the world have warned the company for many years that its money transfer system was being used to

perpetrate consumer frauds, and that Western Union was not adequately addressing the problem.

50. First, in or around 2002, multiple state Attorneys General issued subpoenas to Western Union in conjunction with their investigations of the use of Western Union's money transfer system by fraudulent telemarketers. In correspondence dated October 1, 2002, the Vermont Attorney General's Office informed Western Union about disturbing statistics regarding telemarketers in Quebec, Ontario, British Columbia, and Israel misusing Western Union's money transfer system for frauds.

51. In or around November 2005, Western Union entered into an agreement with forty-seven states and the District of Columbia involving the use of Western Union's money transfer system by "fraudulent telemarketers in and outside the United States" ("2005 Agreement"). The 2005 Agreement imposed a number of requirements upon Western Union, including warnings to consumers, agent training, closure of agents, development of a computerized system to identify likely fraud, and increasing anti-fraud staff. For example, the 2005 Agreement required that Western Union "terminate those of its agents, subagents or locations, as the case may be, who are complicit in fraud-induced transfers or who knowingly ignore such fraud, or, if certain employees of the agent or subagent are the complicit or knowingly ignoring parties, insist upon termination of such employees

as a condition to continued agent or subagent status.” The 2005 Agreement was in effect for five years. Despite this agreement, as explained below, Western Union in many instances failed to terminate many problematic agent locations, especially in countries outside of the United States and Canada.

52. In October 2009, the FTC announced that it had reached a settlement with MoneyGram International, Inc. (“MoneyGram”), Western Union’s main competitor, relating to charges that the company had allowed its money transfer system to be used for fraud. The FTC publicly released copies of the complaint and order against MoneyGram, which required, among other things, the termination of any agent that “may be complicit in” fraud. Following the FTC’s settlement with MoneyGram, FTC staff sent a letter to Western Union in November 2009 expressing concern about the “huge volume of fraud that employs money transfer services,” like that of Western Union.

53. According to Western Union’s records, in or around September 2010, the Japan Financial Services Agency expressed concerns about Japanese consumers sending fraud-induced money transfers to the UK, and “suspicious viewing/surfing of transactions in the United Kingdom, resulting in either Paid in Error (PIE) or Non Payment Claims [complaints about money transfers being paid to the wrong person or not being paid].”

54. Since at least June 2011, the Minnesota Attorney General's Office has been warning Western Union in correspondence directed to the attention of the President and Chief Executive Officer that "each year thousands of consumers are defrauded through use of your company's services," and that "[g]iven your firm's apparently continuing inability or unwillingness to detect and prevent such wire transfer fraud, it would seem appropriate to" issue refunds to consumers. This correspondence has routinely described the consumer complaints the Minnesota Attorney General has received from fraud victims. In response, Western Union typically has refused to issue any refunds to the victims after the funds were paid out.

55. In or around October 2011, multiple state Attorneys General issued subpoenas to Western Union in connection with investigations of fraudulent telemarketers' use of Western Union's money transfer system. The subpoena issued by Vermont stated that it had "reason to believe that Western Union has provided substantial assistance to fraudulent telemarketers in the form of access to its money transfer system, despite knowing, or consciously avoiding knowing, of the fraud, in violation of the Vermont Consumer Fraud Act, 9 V.S.A. § 2453(a)."

56. On or about November 29, 2011, Western Union personnel met with the Korea Financial Supervisory Services to discuss the regulator's concerns about



consumer fraud involving Western Union's money transfer system and its requirement that Western Union put together a plan to alleviate consumer fraud.

57. In February 2012, in response to a survey sent to law enforcement by Western Union, a Special Agent for the U.S. Secret Service warned Western Union of the following: that its services were "widely used by Nigerian scammers and other criminal elements overseas"; "a person in America can easily be robbed by someone in a foreign country and there is almost no possibility to recover that fraud loss"; its "services are widely used for online scams in the US"; and that Western Union "is a complete and almost total safe haven for the criminal element to freely launder illegal proceeds without detection."

58. According to Western Union's records, by the first quarter of 2012, the Serious Organised Crime Agency ("SOCA") in the United Kingdom, presently known as the National Crime Agency, disclosed to Western Union that in relation to an "investigation conducted on money remitters in Western England," SOCA had "surveyed Western Union customers and found that 81% of the transactions paid in Nigeria or Ghana were allegedly fraud related."

59. In or around late May 2012, the Toronto Police Service sent Western Union a letter alerting the company that it "may have aided individuals with the criminal offense of laundering [the] proceeds of crime" from consumer frauds, and cautioning that it needed to take "the appropriate steps . . . to ensure that Western

Union is not a party to this serious criminal offense, whether intentionally or willfully blind to its role.” In numerous additional instances, the Toronto Police Service emailed Western Union information about other fraud-induced money transfers and the names of individuals who had collected the transfers, telling the company to consider the emails a formal caution that allowing the individuals to collect future transfers could be considered “aiding the criminal offence of Laundering the Proceeds of Crime.”

60. In or around October 2012, Western Union received a letter from SEPBLAC, Spain’s Financial Intelligence Unit and Anti-Money Laundering/Counter Financing of Terrorism Supervisory Authority, informing Western Union that an inspection had revealed “extremely serious facts,” which required WUPSIL to “adopt urgent measures in order to correct them immediately,” and that the operations of a “significant part of” Western Union’s agents in two networks owned by Western Union “are related to fraud and money laundering.”

**DESPITE AWARENESS OF THE FRAUD,**  
**WESTERN UNION HAS CONTINUED TO PROVIDE**  
**SUBSTANTIAL ASSISTANCE OR SUPPORT TO CONSUMER FRAUDS**

61. Since at least January 2004, and continuing thereafter, Western Union has been aware that perpetrators of frauds have used its money transfer system to obtain funds from their victims, and for many years has knowingly, or with

conscious avoidance of knowledge, provided substantial assistance or support to fraudulent telemarketers and con artists.

62. In some cases, Western Union's agents, subagents, or FLAs have been complicit, or sometimes even participated, in the frauds. In other cases, Western Union's agents, subagents, or FLAs have offered substantial assistance or support to the frauds by paying out funds in violation of Western Union's own policies and procedures.

63. Western Union has provided an essential service to these fraudulent telemarketers, sellers, and con artists by permitting them access to Western Union's money transfer system. Exploiting this access to its full potential, telemarketing, mass marketing, and imposter scams have received, and continue to receive, millions of dollars from victimized consumers, while generating substantial revenue for Western Union from transaction fees and foreign currency exchange fees.

64. For many years, Western Union has failed to: (a) promptly investigate, suspend, and terminate potentially complicit agents and subagents, or agents and subagents that have failed to comply with Western Union's anti-fraud and/or AML policies and procedures; (b) conduct adequate due diligence on prospective and existing agents and subagents; (c) effectively train, monitor, and review its agents, subagents, and FLAs; (d) adequately collect, record, and report

consumer fraud involving its money transfer system; and (e) take other reasonable steps to prevent fraudulent telemarketers, sellers, and con artists from using Western Union's money transfer system to perpetrate their frauds.

65. In numerous instances, Western Union has failed to take timely, appropriate, and effective measures to mitigate fraud in connection with its processing of money transfers sent by consumers despite knowledge, or conscious avoidance of knowledge, that: fraudulent telemarketers, sellers, and con artists have extensively accessed and exploited Western Union's money transfer system; Western Union's money transfer system has played an integral role in the scams; and a number of its agents have been complicit, or involved, in the frauds, or have failed to adhere to Western Union's policies and procedures to detect and prevent fraud.

**Western Union Has Failed to Promptly Investigate, Suspend,  
and Terminate Agents with High Levels of Consumer Fraud**

66. Despite Western Union's awareness of consumer fraud involving its system, Western Union has in many instances failed to promptly investigate, suspend, and terminate agents and subagents that have exhibited high levels of consumer fraud, some of which were likely complicit in frauds, or which have ignored such frauds by failing to comply with Western Union's policies and procedures, thereby causing significant and ongoing harm to consumers.

67. Even though Western Union's internal reports have identified agent locations where 5% to over 75% of the transactions (in volume or amount) constituted confirmed and potential fraud, and/or suspicious activities, such as surfing, flipping, and data integrity issues, Western Union has allowed many of these agents and subagents to continue operating, with only temporary suspensions, if any. In many cases, Western Union has simply "escalated," or referred, such agents for further review or investigation, but the investigations often have been delayed for months, and in many instances, the escalations have failed to resolve the problems. Western Union frequently has relied on its master agents to conduct their own investigations of their subagents and locations, but has failed to ensure that the master agents' investigations are adequate. Western Union also has sometimes repeatedly escalated the same agents for review or investigation without suspending or eventually terminating those agents even while the agent has continued to be the subject of fraud complaints. Western Union has sometimes even disregarded recommendations from its employees to suspend or terminate certain agents or subagents due to serious consumer fraud problems.

68. Western Union has permitted agents and subagents that have processed hundreds of thousands of dollars, or even millions of dollars, in confirmed and potential fraud to continue operating for months or even years despite highly suspicious activities and indications of complicity. For example,

one agent location in Spain, Locutorio Okuns, operated from 2005 until at least 2012. During that time, the agent engaged in highly suspicious activity, including making payouts related to 126 complaints totaling at least \$341,771 in reported fraud, and receiving over \$1 million from the United States in money transfers that had characteristics indicative of fraud, such as unusually high-dollar amounts and serious data integrity issues. The agent also displayed highly suspicious spikes in volume that corresponded with spikes in fraud complaints. Although it was reviewed by Western Union at least five times, the agent was permitted to continue to operate for years, and its owner was ultimately one of the individuals arrested by the Spanish police in 2014, as described above. Another agent location in the UK, S S Newsagent, made payouts relating to at least 347 complaints totaling \$924,695 in reported fraud between 2005 and 2012. That agent received over \$2.7 million in money transfers from the United States, including over \$1 million in 2007 alone, and the majority of those transactions had characteristics indicative of fraud, including unusually high-dollar amounts and data integrity issues. Even though the agent was reviewed multiple times, it was not terminated despite its history as a high-fraud agent.

69. Even in instances where Western Union has suspended high-fraud agents after a few months rather than years, the agents often have generated significant consumer losses that Western Union could have prevented by acting

more quickly. These agents frequently are immediately identifiable based on spikes in fraud complaints during the first problematic month. For example, during a 30-day period beginning in December 2011, Western Union received 54 complaints, totaling \$246,746, concerning money transfers paid out at one agent location in Bolivia. This location had a Nigerian owner and had already been reviewed by Western Union in the past due to suspicious activity involving millions of dollars in payouts from China. Western Union failed to promptly suspend the agent and during a roughly four-month period from December 2011 to April 2012, it was responsible for paying out at least 191 transfers associated with fraud complaints totaling \$825,319. The average reported fraud transfer was \$4,321, and all of the complaints involved U.S. senders who were the victims of emergency scams. Although this agent was suspended in July 2012, it had paid out over \$2.5 million in suspected fraud in just over four months before Western Union took action.

70. In instances where Western Union suspended agents or subagents due to consumer fraud, the suspensions often were only temporary, even in high-risk fraud countries, such as Nigeria, Ghana, and Jamaica. For example, in or around 2012, Western Union identified and suspended 13 agent locations in Montego Bay, Jamaica, that had been processing millions of dollars of fraudulent and potentially fraudulent money transfers related to lottery/sweepstakes fraud. The suspensions

only lasted a short time, however, before the agents were reactivated. After being reactivated, ten of those agents have continued to pay out tens to hundreds of reported fraud complaints each year since 2013, and in that span have been the subject of 2,055 complaints totaling \$737,319.

71. In some instances, reactivated agents or subagents were assigned new agent ID numbers or became subagents in different agent networks. For example, Western Union's top fraud payout agent in Mexico made payouts relating to at least 410 complaints totaling over \$1.4 million in reported fraud between March 2011 and July 2012. Western Union finally suspended the location in July 2012, but one month later, the same agent began to operate again under a new agent ID, and it continued generating fraud complaints. In addition, Western Union even reactivated some agents that had been terminated due to consumer fraud.

72. Western Union's general practice has been to attempt to rehabilitate agents and subagents exhibiting high levels of consumer fraud by requiring its agents to implement "action plans" to address the problems, but this practice has been inadequate and ineffective. In many instances, Western Union or its agents have failed to create action plans that effectively address consumer fraud. The action plans also often do not adequately and effectively address problems with agents, subagents, and FLAs who are potentially complicit and/or have engaged in suspicious activities. For example, the action plans frequently call for the training



of agent locations and FLAs even though Western Union has acknowledged that “identifying and eliminating complicit actors from the system is more effective at combating consumer fraud than training.” In other instances, Western Union or its agents have failed to create any action plan or for months have delayed creating action plans. Even after action plans have been created, in some cases, the agents and subagents have resisted implementing them, failed to do so satisfactorily, or even ignored them.

73. For many years, suspensions and/or terminations were typically limited to agents in the United States and Canada. For example, between January 1, 2006 and November 1, 2010, Western Union failed to terminate many problematic agent locations worldwide that had paid out \$100,000 or more in reported fraud, including in the UK (124 agents), Nigeria (56 agents), Ghana (18 agents), Jamaica and Spain (16 agents each). In fact, two UK agents each were responsible for paying out over \$2 million in reported fraud between January 1, 2006 and November 1, 2010. Moreover, as of October 2015, Western Union had rarely, if ever, terminated agent locations for fraud in certain high-risk countries, including, but not limited to, Mexico, Nigeria, Ghana, the Dominican Republic, China, and Haiti, despite high levels of fraud and indications of complicity at agent locations.

### **Western Union Has Failed to Conduct Adequate Due Diligence on Agents**

74. For many years, Western Union has failed to conduct adequate due diligence on its prospective agents and subagents, as well as those agents and subagents whose contracts come up for renewal. Western Union either has not conducted background checks on many of its agents and subagents, or to the extent background checks have been conducted, they often have been inadequate. It also has, in many instances, failed to maintain records demonstrating that it has conducted such background checks. In addition, despite awareness of problems with FLAs, Western Union does not conduct any due diligence on, and frequently knows little about, its agents' and subagents' FLAs.

75. For many years, Western Union has failed to conduct routine background checks of each of its prospective and existing agents and subagents located around the world. Even though Western Union's agreements provide it with the authority to conduct background checks on its agents or subagents at any time, Western Union's practice in many countries has been to rely on its agents to conduct due diligence on their own subagents and FLAs, rather than conduct its own background checks, including of subagents operating in high-risk fraud countries. In some instances, Western Union has approved agents or allowed existing agents to continue operating without even knowing the identities of all individuals with ownership, or beneficial ownership, interests in the agent. In

other instances, Western Union has not known, and has not required its agents to disclose or update, the identities of all of its subagents or FLAs.

76. In numerous instances, background checks conducted by Western Union have not been thorough, consisting only of collecting limited information and conducting some type of credit or financial check, rather than criminal background checks of its agents and subagents. In many cases, Western Union has relied upon inaccurate, incomplete, or false information provided by agents and has failed to verify the accuracy of information provided by applicants. Western Union also has installed agents or subagents with criminal histories, including felonies and misdemeanors involving dishonesty, as well as histories of investigations and lawsuits involving allegations of fraud. For many years, the department at Western Union primarily responsible for conducting background checks has not been provided with sufficient information to conduct thorough background checks of every prospective and existing agent and subagent, such as information from law enforcement, information about investigations of agent locations, and access to consumer complaints.

77. In some cases, Western Union has installed agents or subagents that it had previously terminated, that were previously suspended or terminated by MoneyGram for fraud, or that were concurrently operating as MoneyGram agents (in violation of Western Union's agent agreements). One Western Union agent in

College Park, Georgia, for example, was suspended in 2006 due to consumer fraud, but began operating again in 2007 from the same address, but with a different business name and agent ID number, until it was suspended for fraud again. The agent then became a MoneyGram agent and continued to generate fraud-induced money transfers for approximately one year before being terminated by MoneyGram. After that, the agent returned to Western Union in 2009, and began operating for a third time with the same name and at the same location. A review in 2012 revealed that approximately 80% of its payouts were attributable to fraud, and it was later terminated. In 2015, the agent began operating again as a Western Union agent from the same address, using a similar name, but with a new agent ID number, and once again, it began generating fraud complaints.

78. Western Union's background checks also have failed to prevent previously terminated agents or subagents from using straw men to become agents or owners again to gain access to Western Union's money transfer system. In addition, Western Union has installed as agents or subagents individuals who had previously been interdicted (*i.e.*, blocked from using Western Union's money transfer system) due to suspicious activities, or were former FLAs at agent locations that were suspended or terminated for fraud. For example, after suspending an agent location in the Philippines due to high levels of fraud, Western Union discovered that the owner of the location had been a high-volume

sender to Nigeria who Western Union had interdicted just two months before the location began operating. During the three-month period before the agent location was suspended, it generated at least 173 fraud complaints totaling \$316,400, and paid out over \$1.2 million in suspected fraud.

### **Western Union Has Failed to Effectively Train, Monitor, and Review Agents**

79. For many years, Western Union has failed to effectively train, monitor, and review its agents, subagents, and FLAs to detect and prevent consumer fraud and to prevent potential complicity at agent locations.

80. For many years, Western Union has provided only limited training to agents and subagents with respect to detecting and preventing consumer fraud, and its training overall has been inadequate and ineffective. In many instances, FLAs responsible for processing fraud-induced money transfers at Western Union's agent locations have not been knowledgeable about Western Union's anti-fraud and/or AML policies and procedures, including with respect to detecting and preventing fraud, properly recording customers' biographical information and IDs, and addressing suspicious activities. Western Union also has not had an adequate and effective system in place to ensure that FLAs are knowledgeable in these areas. As a result, in many instances, Western Union's high-fraud agent locations have violated the company's policies and procedures by failing to collect proper IDs or biographical information from recipients of money transfers, accepting

improper forms of IDs, or recording obviously incorrect or fictitious ID information into Western Union's system.

81. Western Union's complaint database shows that its agent locations that have paid out fraud-induced money transfers frequently have permitted fraudsters to pick up money transfers using fake IDs, or without recording IDs or other required information. For example, in many instances, these agent locations have recorded the same IDs for multiple recipients, or different IDs for the same recipients. In addition, for tens of thousands of fraud-induced money transfers, Western Union's records frequently show no birthdates, or facially invalid birthdates, such as "1/1/1900," for the recipients. Western Union's records also show that its agent locations have paid out at least 32,764 money transfers of \$1,000 or more that consumers reported as fraudulent from 2004 through August 2015 without recording any ID information for the recipients.

82. In addition, despite Western Union's 2005 Agreement with the States, which required Western Union to "commence a program of person-to-person or telephone training at agent locations known to have a materially elevated level of outgoing or incoming fraud-induced transfers sent from the United States to anywhere except Mexico," in many cases, and especially with respect to foreign agents and subagents, Western Union failed to comply with this requirement. For example, with respect to many of its foreign agent locations that have exhibited

high fraud levels, Western Union's practice was only to train the master agents and not to conduct person-to-person or telephone training at the agent locations that exhibited high levels of fraud.

83. For many years, Western Union has failed to adequately monitor its agents' activity for fraud. In many instances, Western Union employees responsible for monitoring the activities of agent locations have not been provided with sufficient information or resources to adequately monitor Western Union's agents, subagents, and FLAs. For example, in some instances, Western Union has assigned more than one agent ID number to a single agent or subagent without providing Western Union employees with the means to easily locate all of the agent's or subagent's ID numbers in Western Union's system. Western Union has similarly failed to provide its employees with the means to easily identify agents or subagents with common ownership. In addition, in some cases, Western Union's employees have been unable to identify problematic FLAs because FLAs have not used unique IDs when processing money transfers. Western Union's employees also sometimes have not had complete and historical information about particular agents and subagents, including information about all fraud complaints, prior reviews, investigations, and internal reports related to fraud, as well as transactional activity. Therefore, Western Union employees responsible for monitoring agent activity may not have been aware of all relevant information.

84. Western Union has failed to conduct adequate and routine onsite compliance reviews of its agent locations worldwide. Western Union often has relied on its master agents to conduct reviews, but has failed to ensure that those master agents are conducting adequate and effective oversight of their subagents and locations. In some cases, those agents have not even allowed Western Union employees to visit locations without them being present. In other cases, Western Union's employees have not been able to conduct independent onsite reviews of certain locations because they were in areas considered too dangerous to visit. Western Union also has failed to conduct adequate and routine onsite reviews of many of its independent agents.

85. For many years, consumer fraud was not even routinely addressed in compliance reviews of agents. Even after it was added to the list of topics for these reviews, consumer fraud for many years was addressed only in a cursory manner. In addition, in many instances, Western Union employees who conduct compliance reviews have not been provided with information about fraud complaints received involving the agents being reviewed, so the employees could not adequately address issues related to the complaints in their reviews.



**Western Union Has Failed to Adequately Collect, Record,  
and Report Consumer Fraud Involving Its Money Transfer System**

86. Since at least January 2004, Western Union has maintained a complaint database, which contains information relating to complaints or reports the company receives about fraud-induced money transfers.

87. The information contained in Western Union's complaint database significantly understates the number of actual fraud-induced money transfers and losses reported to the company. Despite receiving information from consumers, their family members, or law enforcement representatives about fraud-induced money transfers, Western Union often has failed to record information about all of those money transfers in its complaint database. In other instances, Western Union has failed to record in its database any of the victims' fraud-induced money transfers.

88. Up until in or around December 2011, Western Union did not provide any toll-free number that consumers in countries other than the United States and Canada could use to report fraud and to try to stop the payout of a fraud-induced money transfer. For example, Western Union did not provide fraud hotlines for consumers in Germany, Mexico, Spain, and the UK until December 2011, for consumers in Australia, Japan, and Malaysia until February 2012, and for consumers in Austria, Belgium, Luxembourg, and Switzerland until August 2012.

89. Western Union uses the information in its complaint database to administer its anti-fraud program, so it is important that the database be accurate and complete. For example, Western Union uses this information to: (a) monitor and identify agents, subagents, and FLAs that may be complicit in frauds; (b) create automated rules regarding particular corridors (*e.g.*, limiting the number and amount of money transfers to receivers); and (c) interdict individuals who are the victims or the perpetrators of frauds. Therefore, Western Union's failure to keep accurate and complete records of fraud-induced money transfers has impeded its efforts to detect and prevent consumer fraud.

90. Although Western Union employees have brought the underreporting of fraud-induced money transfers in the company's complaint database to the attention of those responsible for maintaining the database, Western Union has failed to take adequate corrective action, if any, to address the problem.

91. Although the Financial Crime Enforcement Network ("FinCEN"), the primary administrator of the BSA, requires money services businesses like Western Union to file Suspicious Activity Reports ("SARs") relating to fraud, Western Union has, in many cases, failed to file SARs on, and identify as the subject of SARs, particular agent locations in foreign countries that have processed high levels of fraud-induced money transfers sent by U.S. consumers and exhibited other suspicious activities.

**Western Union Has Failed to Take Other Reasonable Measures to Mitigate Fraud in Connection With Its Processing of Money Transfers**

92. For many years, Western Union has failed to take other reasonable measures to mitigate fraud in connection with its processing of money transfers, ignoring in some instances useful suggestions and recommendations from its employees and representatives of law enforcement agencies. These types of measures include, but are not limited to, the following: bolstering its ID requirements for sending or receiving money transfers, such as by imposing more robust ID requirements; requiring the collection of additional biographical information; implementing more controls for noncompliant transactions or potentially fraud-induced money transfers, including, but not limited to, transactions with data integrity issues and to high-risk countries; improving the company's handling of, and ability to receive, complaints about fraud worldwide; and improving its interdiction system to be more effective in blocking money transfers associated with consumer fraud, including, but not limited to, by permanently blocking payouts to the recipients of fraud-induced money transfers.

93. Western Union has made it difficult for employees to take meaningful action to detect and prevent consumer fraud, including by failing to provide employees with sufficient information or resources, including complete records of consumer fraud complaints, as well as information about law enforcement contacts, investigations, and actions. For many years, departments within Western

Union responsible for handling consumer fraud issues did not routinely share consumer fraud information with other groups or departments.

94. Although Western Union relies on its agents to comply with Western Union's anti-fraud and AML programs, and to oversee the activity of their own subagents, locations, and FLAs, it often fails to provide its agents with the information necessary to conduct effective fraud reviews and to detect and prevent consumer fraud, including the potential complicity of particular agent locations and FLAs. For example, Western Union typically does not share with the agents themselves complaints it has received about fraud-induced money transfers processed by the agent locations or FLAs. Therefore, despite being tasked with overseeing the conduct of their own subagents, locations, and FLAs, Western Union's agents in many cases are unaware of the nature, details, history, and volume of complaints involving the agent locations and FLAs.

95. Western Union and its agents also have failed to provide adequate and effective warnings to consumers about the fraud occurring through its money transfer system. Although Western Union provides some warnings on the first page of send forms located at some of its agent locations, in many cases, these warnings are not clear and conspicuous to many consumers. In addition, Western Union's agent locations have failed to provide routine verbal warnings to consumers before they initiated money transfers, even in instances where

consumers' money transfers have displayed obvious signs of fraud, such as high-dollar money transfers by elderly consumers to countries known for fraud.

Therefore, consumers often have been unaware of the risks associated with sending money through Western Union's money transfer system.

**WESTERN UNION HAS FOR MANY YEARS FAILED  
TO MAKE EFFECTIVE CHANGES TO PREVENT FRAUD**

96. Even after January 2011, when Western Union claimed in a written report to have implemented "a comprehensive anti-fraud program" to protect consumers, Western Union still failed to adopt an adequate and effective anti-fraud program. Although as a result of the FTC's investigation, Western Union has improved aspects of its anti-fraud program since 2012, the company still failed in certain cases to promptly terminate agents around the world that appeared to be complicit in paying out the fraud-induced money transfers, including numerous agents in Spain that operated between January 2011 and December 2012, and were arrested by the Spanish police in 2014 for their role in laundering large sums of money received from the fraud victims. As of October 2015, Western Union had rarely, if ever, terminated agent locations for fraud in certain high-risk countries, including, but not limited to, Mexico, Nigeria, Ghana, the Dominican Republic, China, and Haiti, despite high levels of fraud and indications of complicity at agent locations.

97. In numerous instances, Western Union has permitted agent locations to continue operating for months or years despite high levels of fraud and other suspicious activities. For example, from July 2009 to as recently as August 2015, an agent location in Malaysia made payouts relating to at least 252 fraud complaints totaling \$389,061. Although the agent appeared on fraud reports and was reviewed for fraud many times between 2010 and 2014, the agent has not been terminated. In fact, in 2014, company executives approved the reactivation of that agent despite being informed that confirmed and potential fraud, as well as suspicious activity, amounted to approximately 54% of the agent's pay volume. An agent location in Greece made payouts relating to at least 106 fraud complaints totaling \$193,696 from July 2013 to October 2014. From 2012 to 2014, the agent paid out \$5.4 million in money transfers, of which approximately \$3.7 million were for \$1,000 or more. That agent operated for over two years despite appearing on internal fraud or agent complicity index reports multiple times and being reviewed for fraud at least three times with findings of suspicious activities. From September 2013 to August 2015, an agent in Thailand paid out money transfers associated with at least 1,197 complaints totaling \$425,409, of which 336 complaints totaling \$117,290 were paid out in April 2015 alone. That agent was allowed to continue operating, despite a review in 2013 finding that 63% of the agent's transactions in two months amounted to confirmed fraud and questionable

activity, and a review in 2015 associated with three of its agent ID numbers finding that 25% of its activity in one month, amounting to over \$1.2 million, was connected to fraud.

### **VIOLATIONS OF THE FTC ACT**

98. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits “unfair” or “deceptive” acts and practices in or affecting commerce, including acts or practices involving foreign commerce that “cause or are likely to cause reasonably foreseeable injury within the United States” or “involve material conduct occurring within the United States.”

99. Acts or practices are unfair under Section 5 of the FTC Act if they 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**

#### ***Unfair Acts or Practices***

100. In numerous instances, in operating its worldwide money transfer system, Defendant has failed to take timely, appropriate, and effective action to detect and prevent fraud-induced money transfers through Defendant’s system, as described above.

101. Defendant's actions 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.

102. Therefore, Defendant's practices as described in Paragraph 100 above constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. §§ 45(a) and 45(n).

### **THE TSR**

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

104. Defendant, its agents, or subagents have processed money transfers and provided related services on behalf of persons who are "sellers" or "telemarketers" engaged in "telemarketing," as those terms are defined in Sections 310.2 (dd), (ff), and (gg) of the TSR.

105. The TSR prohibits telemarketers and sellers from making a false or misleading statement to induce any person to pay for goods or services. 16 C.F.R. § 310.3(a)(4).



106. The TSR also prohibits telemarketers and sellers from, among other things, requesting or receiving payment of any fee or consideration in advance of obtaining a loan or other extension of credit when the seller or telemarketer has guaranteed or represented a high likelihood of success in obtaining or arranging a loan or other extension of credit. 16 C.F.R. § 310.4(a)(4).

107. It is a violation of the TSR for any person to provide “substantial assistance or support” to any seller or telemarketer when that person “knows or consciously avoids knowing” that the seller or telemarketer is engaged in any act or practice that violates Sections 310.3(a), (c), or (d), or 310.4 of the TSR. 16 C.F.R. § 310.3(b).

108. On December 14, 2015, the FTC published a notice that it had adopted amendments to the TSR, including a prohibition against using “cash-to-cash” money transfers for outbound and inbound telemarketing transactions. 80 Fed. Reg. 77520 (Dec. 14, 2015). This prohibition became effective on June 13, 2016.

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

**VIOLATIONS OF THE TSR**

**COUNT II**

*Assisting and Facilitating TSR Violations*

110. In numerous instances, in the course of processing money transfers, Defendant, its agents, or subagents have provided substantial assistance or support to sellers or telemarketers who Defendant or its agents or subagents knew or consciously avoided knowing:

- a. Induced consumers to pay for goods and services through the use of false or misleading statements, including, without limitation, the statement that the consumer has won and will receive a large cash award if the consumer pays a requested fee or fees, in violation of Section 310.3(a)(4) of the TSR, 16 C.F.R. § 310.3(a)(4); and
- b. Requested or received payment of a fee or consideration in advance of consumers obtaining a loan when the seller or telemarketer has guaranteed or represented a high likelihood of success in obtaining or arranging a loan for a person in violation of Section 310.4(a)(4) of the TSR.

111. Defendant's acts or practices, as described in Paragraph 110 above, constitute deceptive telemarketing acts or practices that violate the TSR, 16 C.F.R. §310.3(b).

### **CONSUMER INJURY**

112. Consumers have suffered and will continue to suffer substantial injury as a result of Defendant's violations of the FTC Act and the TSR. In addition, Defendant has been unjustly enriched as a result of its unlawful acts or practices. Absent injunctive relief by this Court, Defendant is likely to continue to injure consumers, reap unjust enrichment, and harm the public interest.

### **THIS COURT'S POWER TO GRANT RELIEF**

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

### **PRAYER FOR RELIEF**

114. WHEREFORE, Plaintiff, the Federal Trade Commission, pursuant to Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), Section 6(b) of the Telemarketing

Act, 15 U.S.C. § 6105(b), and the Court's own equitable powers, requests that the Court:

1. Enter a permanent injunction to prevent future violations of the FTC Act and the TSR by Defendant;
2. Award such relief as the Court finds necessary to redress injury to consumers resulting from Defendant's violations of the FTC Act and the TSR, including, but not limited to, rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies; and
3. Award Plaintiff the costs of bringing this action, as well as such other and additional relief as the Court may determine to be just and proper.

Dated: January 19, 2017

Respectfully Submitted,

DAVID C. SHONKA  
Acting General Counsel



KAREN D. DODGE (IL 6204125)  
JOANNIE T. WEI (IL 6276144)  
ELIZABETH C. SCOTT (IL 6278075)  
Attorneys for Plaintiff  
Federal Trade Commission  
55 West Monroe Street, Suite 1825  
Chicago, Illinois 60603  
(312) 960-5634 (telephone)  
(312) 960-5600 (facsimile)  
[kdodge@ftc.gov](mailto:kdodge@ftc.gov) (Dodge)  
[jwei@ftc.gov](mailto:jwei@ftc.gov) (Wei)  
[escott@ftc.gov](mailto:escott@ftc.gov) (Scott)

NEW YORK STATE DEPARTMENT  
OF FINANCIAL SERVICES

In the Matter of

WESTERN UNION FINANCIAL SERVICES, INC.

**CONSENT ORDER UNDER  
NEW YORK BANKING LAW §§ 39 and 44**

The New York State Department of Financial Services (the “Department”) and Western Union Financial Services, Inc. (“Western Union” or the “Company”) are willing to resolve the matters described herein without further proceedings.

**WHEREAS**, Western Union is a global financial institution and money services business headquartered in Englewood, Colorado, that, together with its affiliates, employs approximately 10,000 people worldwide and has assets of more than \$9.4 billion;

**WHEREAS**, the Company is licensed by the Department to operate a money transmission business in New York State;

**WHEREAS**, in 2016, Western Union agents in New York State processed more than 18 million consumer-to-consumer money transfers, totaling in excess of \$4 billion; this volume accounted for approximately 10 percent of all Western Union money transfers effectuated in the United States.

**WHEREAS**, the Department has been conducting an investigation of Western Union’s money services business. The Department hereby finds as follows:

## The Department's Findings After Investigation

### Introduction

1. The Department has been conducting an investigation of Western Union, including reviewing thousands of pages of documents obtained from the Company and obtaining information from third party sources.

2. Under New York law, Western Union must establish, implement, and maintain an effective anti-money laundering ("AML") compliance program that, among other things, provides for: internal policies, procedures, and controls to guard against money laundering; an individual or individuals to coordinate and monitor day-to-day compliance with the federal Bank Secrecy Act ("BSA"), and New York banking laws and regulations; an employee training program; independent program testing; customer identification verification; and accurate, complete and timely reports of suspicious activity.

3. One way that criminals and other bad actors may utilize money transmitters for improper purposes is to send money illicitly through the practice of "structuring." "Structuring" occurs when a party executes financial transactions in a specific pattern, like breaking up a larger sum into smaller transactions. The purpose of structuring typically is to avoid (a) triggering the obligation of a money transmitter like Western Union to file reports with the federal government required by the BSA, or (b) the money transmitter's own requirements for providing certain types of identification and other evidence of the legitimacy of the financial transaction.<sup>1</sup> New York laws and regulations require money transmitters like Western Union to maintain effective controls to combat structuring by its agents or customers.

---

<sup>1</sup> See, e.g., Internal Revenue Service, Internal Revenue Manual Part 4 ([https://www.irs.gov/irm/part4/irm\\_04-026-013](https://www.irs.gov/irm/part4/irm_04-026-013)).

4. Western Union failed to satisfy this obligation for many years. Between 2004 and 2012, Western Union willfully failed to implement and maintain an effective anti-money laundering program that was designed to deter, detect, and report on criminals' use of Western Union to facilitate fraud, money laundering, and structuring schemes. Despite having evidence that a substantial number of its agents were engaging in suspicious activity, the Company continued to maintain relationships with suspect but profitable business partners, sometimes bending its own policies and procedures to do so. The conduct involved various Western Union offices and agents located in New York, other states, and around the world.

5. Additionally, several Western Union executives and managers knew about (or willfully ignored) improper conduct involving certain high-volume agents located in New York State as it occurred, yet the Company never disclosed this to the Department. Moreover, even after the United States Department of Justice ("DOJ") launched an investigation of Western Union in 2012, and the Company became aware of the full scope of the misconduct by such high-volume New York agents in early 2015, the Company waited approximately two years to fully disclose this information to the Department.

6. On January 19, 2017, The Western Union Company (the parent of the Department's licensee, Western Union) entered into a deferred prosecution agreement with DOJ, in which, based on conduct occurring between 2004 and 2012, it admitted to the federal criminal offenses of (a) willfully failing to implement an effective anti-money laundering program under the BSA (31 U.S.C. §§ 5318(h), 5322 and regulations thereunder), and (b) aiding and abetting wire fraud (18 U.S.C. §§ 2, 1343) (the "DPA"). On the same day, The Western Union Company settled related civil charges brought by the Federal Trade Commission ("FTC") pursuant to a Stipulated Order (the "FTC Order").

7. Pursuant to the DPA, The Western Union Company agreed to forfeit to DOJ a total of \$586 million for the purpose of “mak[ing] the funds available to compensate victims of the fraud scheme described in the [accompanying] Statement of Facts.” The Western Union Company further “acknowledge[d] that at least \$586 million in consumer fraud proceeds are traceable to transactions” that constituted wire fraud, as described in the DPA’s Statement of Facts (“DPASOF”).<sup>2</sup> See DPA at 8.

8. The Western Union Company also consented to an assessment of a civil monetary penalty in the amount of \$184 million by the United States Financial Crime Enforcement Network (“FINCEN”) for failing to maintain an effective anti-money laundering program. The entirety of this penalty was credited against the payment of the above-mentioned forfeiture to DOJ of \$586 million; in other words, Western Union did not make an additional payment in that amount. Accordingly, all of the money paid in forfeiture was determined to be the proceeds of fraud, which is to be returned to victims via federal restitution mechanisms.<sup>3</sup>

**New York’s Important Role in Western Union’s Business**

9. Western Union operates an electronic network by which consumers can send money to individuals and businesses in the United States and around the world. Western Union provides money transfer services to consumers via approximately 550,000 Western Union agent locations in more than 200 countries and territories. Some agents are individuals or small corporate entities that own or operate an independent business and have a contractual

---

<sup>2</sup> See *U.S. v. The Western Union Company*, 17-CR-00011 (CCC) (M.D. Pa. Jan. 19, 2017).

<sup>3</sup> See “Justice Department Announces Compensation Process for Western Union Fraud Victims With Funds Recovered Through Asset Forfeiture,” <https://www.justice.gov/opa/pr/justice-department-announces-compensation-process-western-union-fraud-victims-funds-recovered> (Nov. 13, 2017).



relationship with Western Union that authorizes the agent to offer Western Union's money transfers to consumers.

10. Western Union earns revenue by charging consumers a fee based on the transfer amount and its destination. The Company earns additional revenue on international transactions sent in one currency and received in a different currency.

11. Western Union pays each agent a commission for each money transfer the agent processes. Western Union may also pay an agent bonuses and other compensation based on transaction volume. The Company can terminate or suspend any agent or agent location for a variety of reasons, but especially compliance reasons.

12. Western Union has held a money transmitter license issued by the Department since 1990. The Department is the sole prudential regulator for Western Union in the State of New York.

13. New York plays an important role in Western Union's business operations, with more than 2,800 agent locations in the State. In 2016, New York agents processed more than 18 million consumer-to-consumer money transfers, totaling in excess of \$4 billion. This volume accounted for approximately 10 percent of all Western Union money transfers effectuated in the United States.

14. Moreover, in 2016, money transfers involving New York agents yielded \$224 million in revenue for Western Union. This resulted in gross profits to the Company of approximately \$50 million.

#### **Prior Compliance Failures at Western Union Uncovered by the Department**

15. The Department previously determined that Western Union suffered from compliance failures involving its anti-money laundering program in general, and its efforts to

prevent structuring in particular. In or about 2002, the Department's predecessor agency, the New York State Banking Department, conducted an examination of the Company and determined that it failed to establish effective procedures to monitor its agents, detect suspicious transactions, and file suspicious activity reports (the "2002 Examination"). One of the key deficiencies that the 2002 Examination uncovered was that Western Union agents were permitting structuring to occur.

16. To resolve the deficiencies identified in the 2002 Examination, in December 2002, Western Union agreed to pay a civil monetary penalty of \$8 million for violations of New York law. The Company also agreed to (a) conduct further reviews to identify suspected structuring, (b) establish enhanced due diligence policies to monitor its agents for AML compliance, and, notably, (c) create protocols for terminating agents who consistently violate AML rules and regulations or compliance policies (the "2002 Agreement").

17. As part of a parallel resolution with FINCEN in 2003, Western Union also agreed to conduct further agent reviews to identify suspected structuring to avoid the filing of Currency Transaction Reports or recordkeeping requirements imposed by 31 C.F.R. § 1010.410,<sup>4</sup> and to "establish an enhanced nationwide due diligence policy to monitor its agents for BSA compliance [, which] shall include . . . terminating such agents that Western Union determines to be in chronic violation of Western Union policies and/or a substantial risk for money laundering."<sup>5</sup>

---

<sup>4</sup> Formerly 31 C.F.R. § 103.33(f).

<sup>5</sup> DPASOF ¶ 55.

**Western Union’s Willful Failure to Maintain An Effective Anti-Money Laundering Program and Its Impact on New York Residents and Consumers**

18. Unfortunately, Western Union did not sufficiently improve its compliance in response to the 2002 Agreement. Although the Company made some initial progress through 2006, nonetheless, between 2004 and 2012, Western Union repeatedly failed to meet its compliance obligations by neglecting to terminate or effectively discipline certain agents, in New York and elsewhere, that Western Union knew or should have known were persistently engaging in illegal behavior, such as assisting structuring and abetting third parties perpetrating consumer fraud.

**Willful Failure to Prevent Structuring and Other Unlawful Conduct – New York “China Corridor” Agents**

19. Many of Western Union’s agents conduct money transmission for customers that wish to send funds abroad. A number of New York agents, for example, conduct large volumes of transactions to Western Union locations in China (“NY China Corridor Agents”).

20. For many years, Western Union knew or willfully ignored the fact that certain NY China Corridor Agents facilitated suspicious transactions on behalf of customers. These agents (referred to herein as “Agent 1,” “Agent 2” and “Agent 3”) were some of Western Union’s largest agent locations in the world by transaction volume – and thus some of the most profitable for the Company.

21. **Agents 1 and 2:** Agent 1, located in lower Manhattan, was a small travel agency that offered Western Union money transmission services. Agent 2, located in the Sunset Park neighborhood of Brooklyn, was a small business that sold wireless cellphone services to consumers, and also offered Western Union money transmission services. Moreover, Agent 1

and Agent 2 were closely linked -- Agent 2 apparently was owned by the spouse of the owner of Agent 1.

22. Despite its small size, between 2004 and 2011 Agent 1 processed more than 447,000 transactions totaling more than \$1.14 billion. Similarly, although a small business entity, between 2005 and 2011, Agent 2 processed more than 302,000 transactions, totaling more than \$600 million.

23. Almost all of the more than \$1.7 billion worth of transfers processed by Agent 1 and Agent 2 together in this time period were transmitted to China. According to federal law enforcement authorities, at least 25 to 30 percent of the transactions processed by Agents 1 and 2 in this time period bore characteristics indicative of structured transactions.<sup>6</sup>

24. Likewise, between 2004 and 2012, Agent 3 processed more than 735,000 transactions, totaling more than \$1.2 billion. Like Agents 1 and 2, most of the transfers processed by Agent 3 were sent to China.

25. The sheer number and size of transactions processed by these agents, which were small independent stores each with a small number of employees, stood out as clear indicators of increased money laundering risk. For example, for Agent 1 to have legitimately processed the number and volume of transactions indicated by its aggregate 2005 Western Union money transfer activity, the agent, a small business in New York City, would have had to process an average of 200 transfers, with an average value of \$2,160, each and every day of the year.

26. Western Union possessed evidence that these agents were failing to meet compliance standards. For example, between 2004 and 2011, the Company conducted almost two dozen compliance reviews of Agents 1 and 2. On each occasion Western Union compliance

---

<sup>6</sup> See DPASOF ¶ 69.

staff found that the employees of Agents 1 and 2 were not complying with certain elements of the BSA or Western Union policy.

27. Shortcomings identified by Western Union's own compliance staff included (a) permitting consumers to apparently structure transactions, (b) failing to file suspicious activity reports in every instance where such a report was required, and (c) failing to have sufficient compliance programs. Western Union's reviews even determined that employees of both Agents 1 and 2 were, in certain instances, entering false data into Western Union's transfer records to aid customers in evading regulatory scrutiny.

28. Strikingly, the compliance officer for Agent 1 admitted to a Western Union investigator that she had accepted a large sum of cash from a consumer for transmission, and had fabricated a series of smaller transactions to circumvent reporting requirements.

29. For years, Western Union failed to adequately respond to improper conduct committed by certain of its agents. During the relevant time period, Western Union had an unwritten policy to suspend an agent location from conducting transactions if that agent location was placed on probation three times. "Probation," as understood by Western Union compliance staff, referred to Western Union's policy of engaging in enhanced reviews of an agent location. Company policies called for problematic agents to face escalating levels of discipline for improper or illegal conduct: from probation, to suspension, and finally termination.

30. Nonetheless, on a number of occasions, Western Union management intervened to obtain more lenient treatment for NY China Corridor Agents, which were some of the Company's highest fee generators. For example, in 2009, Western Union compliance staff circulated information about agents who had been placed on probation multiple times due to negative compliance reviews, a group that included Agent 2. As previously noted, Western

Union had an unwritten policy requiring suspension of an agent location if the agent location was placed on probation three times, with “no appeal.”

31. Apparently to reduce the chance that less-compliant agents (such as Agent 2) would again be identified as policy violators, a Western Union compliance employee explained by e-mail to a business executive that compliance staff would give “*plenty of notice before they conduct reviews with agents who have 2 or more probations,*” apparently maximizing the chance for such agents to avoid more serious discipline, and a corresponding suspension or cessation of fee revenue.

32. An executive in charge of business planning for the U.S. Northeast region made extra efforts to shield Agent 2 because of its significance to Western Union business, asking in an e-mail that other business staff “help [the] compliance group understand how important those Chinese agents are – *not shut them down automatically. [Agent 2] is [the] #2 agent in the region and we can't afford [a] one week suspension.*”

33. Similarly, in approximately 2008, Agent 1’s owner had been exempted from Western Union’s policy of being suspended after accruing multiple negative compliance reviews, given the very large dollar volume of transactions conducted for Western Union. Indeed, rather than suspend the agent for these multiple violations, Company management actually paid Agent 1’s owner a \$250,000 bonus to renew the contract with Western Union.

34. Later, in 2010, Western Union’s then-Director of Compliance reported to Western Union’s then-Chief Compliance Officer (“WU CCO”) that a compliance review of Agent 1 had uncovered numerous additional legal and policy violations. These included the incident discussed above (¶ 28), where Agent’s 1’s compliance officer admitted fabricating consumer transaction records to conceal a customer’s illegal structuring activity. The Director of

Compliance reported to the WU CCO that these new findings warranted suspension of Agent 1, which would constitute Agent 1's third compliance-related suspension.

35. Western Union's business management intervened to ensure that only a short suspension of 24 days was imposed on Agent 1. Moreover, Agent 1's internal compliance officer, who had admitted falsifying records, was permitted to remain in that position and continue to processing voluminous Western Union transfers.

36. Only a few months later, Western Union compliance staff identified a series of additional violations of anti-money laundering policies committed by Agent 1. A compliance officer stated that, under Western Union's policies, this warranted suspension of the agent, given the accrual of negative compliance reviews. No suspension occurred, however, and another compliance staffer noted that this result was a so-called "policy exception."

37. In light of this history, Western Union compliance staff subsequently sought means, other than their own internal disciplinary processes, to address ongoing compliance issues with Agent 1. In 2011, upon obtaining evidence from a former employee of Agent 1 that Agent 1 was potentially involved in criminal activity, Western Union compliance staff discussed bypassing internal processes altogether and referring the matter directly to law enforcement. "In this case," a senior compliance officer wrote in an e-mail to a colleague, "*rather than fighting with the business to gain support to suspend, etc., we thought that [a] better tactic would be to give law enforcement a crack at it.*"

38. Later in 2011, the bank that held direct deposit accounts for Agents 1 and 2 asked Western Union for information about these (and other) agents' compliance programs and Company reviews. Western Union initially resisted this request, fearful that the bank would close the deposit accounts and imperil Western Union's lucrative relationship with these agents.

One Company sales executive told colleagues in an e-mail that responding frankly risked Western Union's agency relationships, and asked whether the Company could conceal what it knew about these agents from the bank:

*Closing [Agents 1 and 2] at this time will impact the US-China corridor BADLY. Please see if there is anything we can do (like verify that [Agent 1] has done something 'not compliant' and [promising to] re-educate Agent 2 to be compliant) and to re-open them in a few weeks to catch the Chinese New Year rush.*

Subsequently, in December 2011, Western Union terminated Agents 1 and 2.

39. The seriousness of the misconduct detected at Agent 1 by Western Union was subsequently confirmed, when Agent 1's owner admitted to law enforcement agents that he knew at least some consumers used Western Union's money transfer services to pay debts to human traffickers based in China, and that consumers would structure transactions to keep them under \$2,500, in order to avoid having to provide identification.<sup>7</sup>

40. Despite Western Union's knowledge of illegal and improper activity at Agent 1, Western Union almost never filed a SAR about Agent 1's own suspicious conduct (filing only two over the span of a decade) -- even though the Company had filed many thousands of SARs regarding particular consumer transactions processed by Agent 1.

41. **Agent 3:** Western Union's relationship with Agent 3 also demonstrates the Department's concerns with Western Union's conduct in this matter. In January 2011, for instance, Western Union's compliance review of Agent 3, which was located in the Flushing neighborhood of Queens, raised serious questions as to whether the agent was allowing structuring activity to occur. The information received included the occurrence of multiple transactions on a particular date without a corresponding quantity of customer traffic. Based on this and other information, a senior employee in Western Union's Global Monitoring and

---

<sup>7</sup> DPASOF ¶ 71.



Intelligence (“GMI”) division explained that these revelations, coupled with prior intelligence, indicated that this agent was a significant compliance risk and recommended that Western Union take “immediate action to mitigate the risk.” Further discussions involving a senior lawyer in Western Union’s compliance group led the compliance team to decide that the Company should terminate its relationship with this agent. The senior lawyer asked that a memo be prepared “*so that I can go to the business and explain what we’ve done. . . . [I] want to ensure the business understands this is not a first time thing or that rehabilitation is an option.*”

42. Later the same day, the senior compliance lawyer reported to her team by e-mail that the business side rejected termination of Agent 3 due to its revenue-generating significance:

*[A business executive with whom she spoke] is not going along with termination. Agent is too significant to the business. I explained the [serious compliance] issues . . . but all he sees is the volume and Chinese New Year.”*

Agent 3 was suspended only for a short period of time, despite the compliance concerns.

43. Not long after, in February 2011, GMI staff reported that, after further investigation, the GMI staff was comfortable lifting Agent 3’s suspension, as some of the underlying information initially relied upon by the compliance team had turned out to be inaccurate. Nevertheless, a GMI official noted that Western Union would subject Agent 3 to “a specially designed AML Compliance Probation . . . as a condition of reactivation.” The official warned: “*With that said, this location is still at risk . . . and a reactivation does present financial and reputational risk to Western Union.*”

44. Less than six months later, in July 2011, compliance staff identified new compliance issues at Agent 3. An analyst noted that the team had discovered a series of transactions processed by Agent 3 that were sent within minutes of each other -- many of which were sent by different people, but all of which were directed to the same recipient in China. This

“many-to-one” pattern may be an indicator of illegal structuring. The analyst noted that many of the transactions were specifically crafted to avoid triggering various enhanced scrutiny or reporting requirements imposed by the Company or state and federal law.

45. A Western Union investigator also reported that, during five different site visits to Agent 3 over the course of two weeks, the investigator witnessed Agent 3 employees permitting (and in some cases, encouraging) customers to structure large transactions by enlisting friends or relatives to assist, and then dividing the larger transactions into smaller ones, so as to keep their transactions below the limit at which Western Union’s enhanced customer due diligence review would apply. The investigator further reported that he informed Agent 3 this was not permissible, and that the agent’s employees should convince customers to combine split transactions and undergo Western Union’s enhanced customer due diligence.

46. The Western Union investigator also reported that he witnessed other compliance shortcomings at Agent 3, including permitting customers to use a photocopy of an identification document instead of an original. Additionally, it was subsequently determined by the compliance team that Agent 3 had failed to file SARs that compliance had asked Agent 3 to file.

47. As the Compliance team then weighed suspending Agent 3 once again for compliance deficiencies, business interests objected to any action that would curtail revenues from this highly profitable agent:

*[Agent 3] is our top location to China in the entire United States. Please note that we need to work together to keep this agent active while still satisfying our compliance requirements.*<sup>8</sup>

---

<sup>8</sup> Western Union’s compliance deficiencies in connection with China Corridor agents reached beyond those located in New York. Between 2004 and 2012, for example, customers of other Western Union China Corridor agents illegally structured hundreds of millions of dollars in transactions to China. See DPASOF ¶ 63.

48. Eventually, Agent 3 provided to Western Union the compliance information that was requested. Western Union has represented to the Department that it has had no serious compliance issues with Agent 3 since 2012, even though it continues to be a high-volume agent,

**By Failing to Exercise Reasonable Supervision Over Its Agents,  
Western Union Aided and Abetted Fraudulent Schemes  
Perpetrated Against Consumers in New York and Elsewhere**

49. Between 2004 and 2012, Western Union aided and abetted various unlawful fraud schemes by failing to exercise reasonable supervision over agency locations that knowingly facilitated fraudulent schemes. These schemes were directed at consumers in the United States and around the world, and likely including residents of New York.

50. Criminals relied on Western Union's money transfer system to facilitate payments from victims of fraudulent schemes to perpetrators around the world. Western Union's conduct, including its failure to take effective corrective actions in a timely fashion, contributed to the success of the fraudsters' schemes.

51. Fraudsters contacted victims by phone, mail, or the internet, inducing them to send money via Western Union by, *inter alia*, (a) promising large cash prizes or sweepstakes winnings in exchange for up-front payments; (b) offering expensive items for sale; (c) promising moneymaking opportunities in return for an advanced payment; and (d) posing as the victim's relative and claiming to urgently need money.

52. These criminals directed victims to send advance payments to fictitious payees via Western Union. Fraudsters obtained payment details from the victim and used them to claim the money. Some Western Union agents were in on the scheme, helping to conceal the identity of the fraudster in exchange for a share in the proceeds.

53. Western Union became aware of many of these fraudulent payments because a number of victims reported the fraud to the Company. Western Union maintained a database with details of all the fraud reports by consumers, using that information to track and investigate agent locations that paid out victims' payments to fraudsters.

54. Between 2004 and 2012, Western Union identified more than \$500 million in reported consumer fraud transactions sent through Western Union agents – a sum that represented only a portion of the total amount of fraud, as many victims did not report fraud to Western Union.<sup>9</sup>

**Western Union Failed to Make  
Timely Supervisory Disclosures to the Department**

55. As the prudential regulator for money transmitters such as Western Union and other financial institutions, the Department relies on transparency from its licensed entities about their financial condition, compliance adequacy, market conduct, and transactions with New York consumers. Licensed financial institutions must observe a duty of prompt and complete disclosure of improper conduct to the Department about which it knows or discovers, including misconduct engaged in by the entity itself, including through employees and agents.

56. With such transparency, the Department is able to help ensure the safety and soundness of such institutions; protect consumers from abusive conduct; and determine that institutions are in compliance with New York laws and regulations.

---

<sup>9</sup> Additional serious and long-term deficiencies in its BSA/AML compliance were identified in the DPA (*see* DPASOP ¶¶ 55-99).

57. Moreover, and just as essential, information obtained from one licensee may assist the Department in supervising other licensees in that category of financial institution and/or in the same vicinity as the subject licensee.<sup>10</sup>

58. Here, at a minimum, several senior Western Union executives and managers knew about (or ignored) improper conduct involving NY China Corridor agents as it occurred. The compliance issues regarding agents stretched back as far as 2004 – close in time to the 2002 Agreement between the Department and Western Union, which involved similar misconduct by certain New York agents. Western Union was thus fully on notice that it needed to keep a watchful eye for agent misconduct in this State.

59. Moreover, Western Union's lack of disclosure to the Department of its prior knowledge concerning NY China Corridor Agents continued after DOJ commenced its investigation of the Company in 2012. Following receipt of grand jury subpoenas from DOJ, Western Union responded (through counsel) to DOJ's investigation for a period of four years, including providing DOJ historic documents, and making periodic presentations to DOJ about Western Union's prior conduct, in an effort to mitigate the consequences of the conduct uncovered.

60. No later than early or mid-2015, Western Union was in a position to disclose its understanding about NY China Corridor Agents to the Department, as it had done with DOJ. No such disclosure was made; instead, the Company provided to the Department only non-specific

---

<sup>10</sup> Disclosure obligations of licensed money transmitters such as Western Union are clearly set forth in the New York Banking Law and its regulations. For example (and without limitation): (a) money transmitters are obligated to submit a report to the Superintendent immediately upon discovering fraud, dishonesty, making of false entries or omission of true entries, or other misconduct, whether or not a criminal offense (3 N.Y.C.R.R. §§ 300.1(a), 406.10(c)); and (b) money transmitters are obligated to submit a report to the Superintendent of incidents that appear to relate to a plan or scheme that would be of interest to other money transmitters or licensed entities located in the same area (3 N.Y.C.R.R. §§ 300.4, 406.10(c)).

reports that merely cited the pendency of federal investigations identified in the Company's public filings with the U.S. Securities and Exchange Commission.

61. The first time that the Department learned of the extent of the conduct engaged in by Agents 1, 2 and 3 was in March 2017 – and only after the Department requested a presentation by the Company on compliance issues affecting Western Union's New York State operations based on the information gathered by the Company during the DOJ investigation.

62. By withholding this information, Western Union deprived the Department of its ability to effectively supervise the Company. Additionally, the Department would have been able to employ this information in supervising other money transmitters with agents in the same or nearby vicinity, and with other licensed financial institutions that interacted with those money transmitters. Further, the Department would have had the ability to analyze the underlying data to uncover broader trends of structuring, money laundering and other illicit financial transactions. None of this occurred when Western Union failed to timely disclose this information to the Department.

**Remediation Undertaken By Western Union**

63. The Department acknowledges that, since 2012, Western Union has undertaken significant remedial measures, and implemented compliance enhancements, to improve its anti-fraud and anti-money laundering programs. Western Union has informed the Department of these remedial and compliance measures, which include (but are not limited to):

- a. between 2013 and 2015, an increase in the number of employees in The Western Union Company's Compliance Department by more than 100 percent, and an increase to the Compliance Department budget of more than 60 percent;
- b. creation of Western Union's Fraud Risk Management Department in 2012, which instituted global agent oversight standards to identify and investigate any agent worldwide that processed a certain number of reported fraud

- transactions, along with new compliance procedures to increase compliance authority and accountability, including with regard to Agent oversight;
- c. hiring a new Chief Compliance Officer and other senior compliance staff in 2013. The Chief Compliance Officer was given a direct reporting line to the Chairperson of the Compliance Committee of The Western Union Company Board of Directors;
  - d. creating new compliance procedures to increase compliance authority and accountability, including with regard to agent oversight. In particular, Western Union created a new AML Oversight Committee, which meets regularly and has authority to take corrective action against agents and implement automatic transaction controls such as Real Time Risk Assessment (“RTRA”) rules.
  - e. empowering employees in eight departments to suspend Agents based on analyses, on-site observations, and/or investigation results, and implementing explicit decision procedures and timelines for agent oversight actions, including corrective action;
  - f. creating new teams within its Financial Intelligence Unit to work with law enforcement and generate internal information for agent and consumer analysis, including a Global Rapid Response Team to reach out to law enforcement proactively with investigative results related to crisis events and Strategic Intelligence Units to identify emerging criminal typologies;
  - g. creating and expanding its Courtesy Call Back program, under which certain potentially fraudulent transactions are held while Western Union contacts the sender to determine whether the transaction is legitimate; and
  - h. expanding fraud reporting mechanisms, including international hotlines, which assist consumers outside the United States in reporting fraud scams to Western Union.

64. Moreover, the Department further recognizes that Western Union has made and continues to make substantial contributions to law enforcement efforts through its continuing cooperation with law enforcement authorities in New York and elsewhere. In setting forth the agreed-upon remedies and relief set forth below, the Department has given positive consideration (among other factors) to the factors set forth in Paragraphs 63 - 64.

\* \* \* \*

65. **NOW THEREFORE**, to resolve this matter without further proceedings pursuant to the Superintendent's authority under Sections 39 and 44 of the Banking Law, the Department and Western Union stipulate and agree to the terms and conditions below:

**VIOLATIONS OF LAW AND REGULATIONS**

66. Western Union failed to maintain an effective and compliant AML program, in violation of 3 N.Y.C.R.R. § 417.2.

67. Western Union failed to exercise reasonable supervision over its agents to ensure compliance with applicable laws, rules, and regulations, in violation of 3 N.Y.C.R.R. § 406.3(g).

**SETTLEMENT PROVISIONS**

**Monetary Payment**

68. Western Union shall pay a civil monetary penalty to the Department pursuant to Banking Law § 44 in the amount of \$60,000,000. Western Union shall pay the entire amount within ten days of executing this Consent Order. Western Union agrees that it will not claim, assert, or apply for a tax deduction or tax credit with regard to any U.S. federal, state, or local tax, directly or indirectly, for any portion of the civil monetary penalty paid pursuant to this Consent Order.

**Remediation**

69. Within 90 days of this Consent Order's effective date, Western Union shall submit to the Department a written plan, acceptable to the Department, that is designed to ensure the enduring adequacy of its anti-money laundering and anti-fraud programs. The plan shall address, at a minimum, the following elements:

- a. maintenance of an independent Compliance Committee of The Western Union Company Board of Directors with oversight of the Chief Compliance Officer and the Compliance Program, including anti-money laundering and anti-fraud programs;



- b. requiring all Western Union agents around the world, regardless of their location, to adhere, at a minimum, to U.S. regulatory and anti-money laundering standards, unless in direct conflict with local law;
- c. implementing a risk-based Know Your Agent program to ensure Western Union agents throughout the world are complying with this plan;
- d. procedures for corrective action, including termination, against agents, including foreign agent locations that process consumer to consumer money transfers conducted through Western Union agents to, from, or through the United States, that the Company has determined pose an unacceptable risk of money laundering or the financing of terrorism, or have demonstrated systemic, willful, or repeated lapses in compliance;
- e. ensuring that, when the Company identifies agent locations in violation of law or Western Union policy and procedures, unless asked to do otherwise by law enforcement, or inconsistent with applicable law, the Company will provide notice to the agent in writing of the nature of the violation; and that the Company will document any training or remedial measures taken by the Company with regard to the violation;
- f. ensuring that all consumer-to-consumer money transfers conducted through Western Union agents to, from, or through the United States, regardless of the origin or destination, are monitored to identify potentially fraudulent transactions;
- g. policies and procedures to ensure that the Company will follow all laws and regulations concerning the filing of Suspicious Activity Reports in the United States for any suspicious activity, as defined by the BSA, its implementing regulations, and New York laws and regulations, including, but not limited to, filing SARs according to regulatory requirements identifying:
  - i. suspicious activity identified by the Company related to consumer to consumer money transfers conducted through Western Union agents of \$2,000 or more (or pursuant to the relevant SAR reporting threshold) to, from, or through the United States, regardless of where in the world the suspicious transactions originate or are received;
  - ii. consumer-to-consumer money transfers conducted through Western Union agents of \$2,000 or more (or pursuant to the relevant SAR reporting threshold) to, from, or through agent locations in the United States that are reported by consumers to the Company as fraud-related, regardless of where in the world the suspicious transactions are received; and

iii. agent location owners, operators or employees anywhere in the world that the Company identifies as engaged in or allowing suspicious activity related to consumer to consumer money transfers conducted through Western Union agents of \$2,000 or more (or pursuant to the relevant SAR reporting threshold) to, from, or through the United States; and

h. ensuring that Western Union provides prompt, complete and accurate information to the Department as required by New York laws and regulations.

70. If applicable SAR reporting thresholds are altered by law or regulation, the Company's policies and procedures shall be modified to conform to any new thresholds, and the plans required by this Order shall be modified accordingly.

**Compliance Point of Contact**

71. Western Union shall designate to the Department a Western Union employee who shall serve as a point of contact with the Department to ensure that Western Union provides, at a minimum, prompt, complete and accurate information to the Department as required by New York laws and regulations. Without limitation, among the information that may be requested by the Department from Western Union includes a written report listing all Western Union agents located in New York State who are in the top five percent of agents in terms of SARs filed by the Company, which includes, for each agent location on the list: (a) information identifying the owner of the agent; and (b) what actions, if any, have been taken with respect to the agent location and/or owner or employees of the agent location and the reason for any such action or lack of action.

**Reports to the Department**

72. At the point of six months, twelve months, eighteen months and twenty-four months after execution of this Consent Order, Western Union shall submit to the Department a

written progress report detailing the form and manner of all actions taken to secure compliance with the provisions of this Order, and the results of any such actions.

**Full and Complete Cooperation of Western Union**

73. Western Union commits and agrees that it will fully cooperate with the Department regarding all terms of this Consent Order. Such cooperation shall include, but not be limited to, Western Union's agreement to request that DOJ and the FTC share with the Department any reports Western Union has provided to DOJ or the FTC pursuant to the DPA and the FTC Order; and providing the Department with copies of any such reports, as requested.

**Breach of Consent Order**

74. If the Department believes Western Union to be in material breach of this Consent Order, the Department will provide written notice to Western Union and the Company must, within ten business days of receiving such notice, or on a later date if so determined in the Department's sole discretion, appear before the Department to demonstrate that no material breach has occurred or, to the extent pertinent, that the breach is not material or has been cured.

75. The parties understand and agree that Western Union's failure to make the required showing within the designated time period shall be presumptive evidence of the Company's breach. Upon a finding that Western Union has breached this Consent Order, the Department has all the remedies available to it under New York Banking and Financial Services Law and may use any evidence available to the Department in any ensuing hearings, notices, or orders.

**Waiver of Rights**

76. The parties understand and agree that no provision of this Consent Order is subject to review in any court or tribunal outside the Department.

**Parties Bound by the Consent Order**

77. This Consent Order is binding on the Department and Western Union, as well as any successors and assigns. This Consent Order does not bind any federal or other state agency or any law enforcement authority.

78. No further action will be taken by the Department against Western Union for the specific conduct set forth in this Consent Order, provided that the Company complies with the terms of this Consent Order.

79. Notwithstanding any other provision contained in this Consent Order, the Department may undertake action against Western Union for transactions or conduct that Western Union did not disclose to the Department in the written materials that Western Union submitted to the Department in connection with this matter.

**Notices**

80. All notices or communications regarding this Consent Order shall be sent to:

For the Department:

For the Department:

James F. Caputo  
Senior Assistant Deputy Superintendent  
for Enforcement  
New York State Department of Financial Services  
One State Street  
New York, NY 10004

Megan Prendergast  
Deputy Superintendent for Enforcement  
New York State Department of Financial Services  
One State Street  
New York, NY 10004

For Western Union:

Caroline Tsai  
Executive Vice President and General Counsel  
Western Union  
12500 East Belford Avenue  
Englewood, CO 80112

Sharon Cohen Levin  
Wilmer Cutler Pickering Hale and Dorr LLP  
7 World Trade Center  
250 Greenwich Street  
New York, NY 10007

**Miscellaneous**

81. Each provision of this Consent Order shall remain effective and enforceable until stayed, modified, suspended, or terminated by the Department.

82. No promise, assurance, representation, or understanding other than those contained in this Consent Order has been made to induce any party to agree to the provision of the Consent Order.

*[Remainder of page intentionally left blank]*


**IN WITNESS WHEREOF**, the parties have caused this Consent Order to be signed this


4 day of January, 2018.

**WESTERN UNION FINANCIAL  
SERVICES, INC.**

By:   
**DARREN A. DRAGOVICH**  
Vice President and Assistant Secretary

**NEW YORK STATE DEPARTMENT OF  
FINANCIAL SERVICES**

By:   
**MARIA T. VULLO**  
Superintendent of Financial Services

By:   
**MATTHEW L. LEVINE**  
Executive Deputy Superintendent for  
Enforcement

# ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Class Action Accuses Western Union of Participating in Wire Fraud](#)

---