IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

FEDERAL TRADE COMMISSION, Plaintiff, v. WALMART INC., a corporation, Defendant.	Case No. 1:22-cv-3372

COMPLAINT FOR PERMANENT INJUNCTION, MONETARY RELIEF, CIVIL PENALTIES, AND OTHER RELIEF

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

1. The FTC brings this action under Sections 5(m)(1)(A), 13(b), and 19 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §§ 45(m)(1)(A), 53(b), and 57b, and the Telemarketing and Consumer Fraud and Abuse Prevention Act ("Telemarketing Act"), 15 U.S.C. §§ 6101-6108, which authorize the FTC to seek, and the Court to order, permanent injunctive relief, monetary relief, civil penalties, and other 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"), as amended, 16 C.F.R. Part 310, in connection with Defendant's failure to take timely, appropriate, and effective measures to detect and prevent fraud in the processing of money transfers sent and received by consumers at its store locations.

SUMMARY OF CASE

2. Money transfers are a common vehicle for fraud. Walmart offers money transfers through its stores, and for many years, consumers have reported tens of millions of dollars

annually in fraud-induced money transfers processed by Walmart employees. These practices have harmed many consumers, including people struggling with debt, those threatened by imposters, and older Americans. Walmart is well aware that telemarketing and other mass marketing frauds, such as "grandparent" scams, lottery scams, and government agent impersonator scams, induce people to use Walmart money transfer services to send money to domestic and international fraudsters. Nevertheless, Walmart has continued processing fraud-induced money transfers at its stores—funding telemarketing and other scams—without adopting policies and practices that effectively detect and prevent these transfers. In some cases, Walmart's practices have even made it easier for fraudsters to collect fraud-induced money transfers at a Walmart store. For example, for years, it was Walmart's policy or practice not to deny payouts to suspected fraudsters at its stores, but instead to have its employees complete those transactions. Even after it became illegal in June 2016 for cash-to-cash money transfers to be used to pay for telemarketing transactions, Walmart failed to take appropriate steps to prevent those types of transfers at its locations. As a result of Walmart's failure Walmart ul0.002hoa2sNsal ore. Fo3

attorneys. 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 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.

DEFENDANT

6. Defendant Walmart Inc., formerly known as Wal-Mart Stores, Inc. ("Walmart"), is a Delaware corporation with its principal place of business at 702 S.W. 8th Street, Bentonville, Arkansas 72716. Walmart transacts or has transacted business in this District, as well as throughout the United States and in other countries worldwide.

COMMERCE

7. At all times relevant 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.

DEFENDANT'S BUSINESS PRACTICES

8. Walmart offers a variety of financial services to its customers at its Customer Service Desks, which are located in all of its stores, and in its MoneyCenters, which are dedicated spaces for financial services located in less than half of Walmart's stores. Walmart's advertisements boast that it is "trusted by millions of customers as their one-stop shop for

with notice about its obligations to detect and prevent consumer fraud at its locations. *FTC v. MoneyGram International, Inc.*, No. 09-cv-6576 (N.D. Ill. Oct. 19, 2009); and *FTC v. The Western Union Company*, No. 17-cv-0110 (M.D. Pa. Jan. 19, 2017).

15. One of the ways in which Walmart's anti-fraud practices have been deficient is in the training of its frontline employees, as well as its supervisors and managers, referred to internally as associates (collectively "employees" or "associates"). In many cases, Walmart has failed to properly train and oversee employees responsible for detecting and preventing consumer fraud involving money transfers at its locations. These deficiencies have included Walmart's failure to provide employees with adequate initial and ongoing training on detecting and preventing consumer fraud, including training about questioning and warning consumers, and rejecting and stopping suspect fraud-induced money transfers. Walmart also failed to ensure that its employees providing money transfer services are knowledgeable about the policies and procedures necessary for detecting and preventing consumer fraud. Until sometime in 2019, Walmart failed to provide any instructions to its employees or warnings to consumers that specifically addressed the June 2016 amendment to the TSR ("TSR Amendment"), which the FTC announced on December 14, 2015. The TSR Amendment prohibits the use of "cash-to-cash" money transfers for goods or services offered or sold through telemarketing or charitable contributions solicited or sought through telemarketing.

16. Walmart has also failed to adequately monitor money transfer activity and address suspicious money transfer activities at its locations, including by employees who have been complacent in detecting and preventing consumer frauds or, in some cases, were engaged in suspicious activities or even complicit in frauds. In many cases, Walmart has facilitated scams by paying out fraud-induced money transfers in violation of its providers' anti-fraud or Anti-Money Laundering ("AML") policies and procedures, or by failing to implement and maintain

its own anti-fraud program designed to detect and prevent consumer fraud at its locations. For example, for many years, Walmart's decision not to train or instruct its employees to deny or reject payouts of money transfers that were suspicious and potentially due to fraud allowed fraudsters to more easily receive payouts of fraud-induced money transfers at Walmart locations. In addition, Walmart has failed to properly train and ensure that its employees are knowledgeable about other basic and important procedures, such as verifying and accurately recording IDs and other customer that

can also initiate money transfers online at Walmart.com or through Walmart's Mobile Express Money Service App and finalize them at a Walmart location. In or around mid-2017, Walmart began installing kiosks at some of its Customer Service Desks and MoneyCenters as an option for consumers to initiate their money transfers. After using the kiosks to stage their money transfers, consumers are required to finalize the transactions at the counter with a Walmart associate.

19. Money transfers sent or received by consumers through Walmart's providers are supposed to be for person-to-person use and not for businesses. Walmart does not limit the maximum amount a consumer can send or receive through a Walmart money transfer. Instead, it relies on its providers to impose the limits. For years, the maximum amount of money that could be sent through MoneyGram at a Walmart location in the United States was $20,000 per day, but the limit for a single transaction was $10,000 until early 2018, when that amount was lowered to $8,000. Originally, the maximum amount that could be sent through a domestic Walmart-to-Walmart money transfer through Ria was $900, but that was raised to $2,500 in October 2016. Until sometime in 2018, generally, there were no set limits on the amount of money that a customer could receive through MoneyGram or Ria in one day. In Canada, the maximum amount of a money transfer that can be sent from a Walmart location is $7,500 (CAD), while the maximum amount that can be received at a Walmart location in Canada is $5,000 (CAD). Regardless of location, consumers sending a money transfer from a Walmart store must pay with cash or a PIN-based debit card.

20. For many years, when initiating a money transfer at a Walmart location, the sender typically was required to complete a "send form," which contained certain consumer fraud warnings. The send form required the sender to provide his or her name, physical address, and telephone number, the name of the recipient, and the state, province and country to which the

complete a "receive form" with the reference number, receive amount, recipient's name, physical address, and telephone number, sender's name, telephone number, and the city and state from which the transfer was sent. The recipient also was supposed to present his or her government-issued photo ID for verification in receiving the transfer, although the Walmart location was only required to record the recipient's ID at a certain dollar threshold. For example, for many years, Walmart was required to record the ID of a recipient who received a money transfer of $900 or more in the United States. In addition, when the recipient did not have an ID and the money transfer was less than a certain amount, such as $900, the sender sometimes had the option of using a preset answer to a test question. For money transfers of $3,000 or more, recipients in the United States also are required to provide their Social Security Number or Tax Identification Number, or if not available, alien ID or passport information to be recorded by the Walmart location. Beginning in or around May 2016, the ID threshold for recipients was lowered to $1, the test question was eliminated, and Walmart stopped using the receive forms.

24. Once the cash funds have been paid out to the recipient, fraud victims usually have not been able to get their money back either from Walmart or its providers. For example, for many years, senders typically could not get their money back unless they had asked for a refund before the money transfer had been picked up. As a result of agreements that MoneyGram and Western Union reached with the FTC, as well as most of the states, between 2016 and 2018, those refund policies have been expanded to provide refunds if the providers or their agents—including Walmart—have failed to follow certain anti-fraud policies and procedures, such as failing to provide the required consumer fraud warnings or to verify or accurately record IDs.

Use of Walmart Money Transfers to Facilitate Fraud and Harm Consumers

25. Walmart has provided an essential service to fraudulent telemarketers, sellers, and con artists by permitting them access to its providers' money transfer systems at its locations while failing to have its own comprehensive and effective anti-fraud program, and, in some cases, failing to comply even with its providers' anti-fraud policies and procedures. Exploiting this access to its full potential, perpetrators of mass marketing and imposter scams have received, and continue to receive, at Walmart locations, millions of dollars from victimized consumers, including many elderly consumers.

26. Fraudulent telemarketers and con artists have preferred to use money transfers at

often have made it easier for victims to unwittingly send money to fraudsters and for fraudsters to receive payments through money transfers at Walmart locations. At the same time, these failures have also made it more difficult for consumers and law enforcement to identify and locate the recipients of fraud-induced money transfers.

27. For years, Walmart has been aware that criminal fraud rings, including those perpetrating telemarketing scams, have picked up fraud-induced money transfers at Walmart. For example, in May 2016, Walmart became aware that individuals had been arrested in connection with an Internal Revenue Service ("IRS") impersonation scam conducted over the telephone that bilked thousands of U.S. consumers out of millions of dollars through fraud-induced money transfers picked up at Walmart locations. Ultimately, at least fifteen individuals were indicted in connection with that scheme, most of whom have since pleaded guilty. *See U.S. v. Caballero*, No. 16-cr-0124 (E.D. Ark.); *U.S. v. Caballero*, No. 16-cr-0201 (D. Minn.), and *U.S. v. Mirabal*, No. 16-cr-0269 (N.D. Tex.); *see also U.S. v. Pando*, No. 17-cr-0046 (N.D. Miss.), and *U.S. v. Labra*, No. 17-cr-0314 (D. Md.). In 2017, Walmart became aware of arrests in at least two other IRS impersonation scams that involved the extensive use of fake IDs at Walmart locations. In one of those scams, four individuals were charged in connection with a scheme that used fake IDs to pick up $66,537 in money transfers from 784 victims from

28. Criminal authorities across the United States have charged other individuals in connection with mass marketing and telemarketing schemes that obtained millions of dollars in fraud-induced money transfers that were sent from or received at Walmart locations. *See*, *e.g.*, *U.S. v. Marcks*, No. 19-cr-0315 (D. Nev.) (five individuals charged in connection with India-based telemarketing and email marketing impostor scam targeting elderly consumers in the U.S. from June 2015 to April 2017 that falsely informed consumers had outstanding taxes, open collection accounts, or other liabilities that required immediate payments to avoid adverse action; at least two defendants have pleaded guilty to conspiring with others in this scheme; internal documents show that Walmart later became aware that this scheme's runners picked up at least 874 fraud-induced transfers totaling over $545,000 at Walmart locations); *U.S. v. Parmar*, No. 19-cr-0160 (E.D. Va.) (six individuals charged in connection with international telemarketing scam involving government impostor and loan scams, including two individuals who pleaded guilty to working with others to pick up millions of dollars in fraud-induced money transfers from U.S. consumers, often at Walmart locations, from at least March 2017 until April 2019); and *U.S. v. Hines*, No. 17-cr-1038 (N.D. Iowa) (six individuals pleaded guilty to involvement in scam that used money transfers to bilk elderly consumers in the U.S. between December 2015 and September 2016; Walmart documents show the scheme used Walmart locations to pick up fraud-induced transfers); *see also U.S. v. Smith*, No. 21-cr-0372 (M.D. Pa.) (two individuals charged in connection with an advance-fee sweepstakes scam conducted from October 2016 to 2018 in which Jamaica-based fraudsters contacted victims by telephone or through the Internet; the defendants regularly received fraud-induced money transfers from multiple Walmart locations, including from multiple Walmart locations in the same day); and *U.S. v. Budhadev*, No. 20-cr-0252 (M.D. Pa.) (individual charged in connection with various India-based mass marketing schemes, including an advance-fee

complaints was approximately $370 from 2013 through 2018. These complaints represent only a small percentage of the actual fraud perpetrated through money transfers sent from or received at Walmart locations.

31. Walmart is responsible for a significant proportion of the complained-about fraud-induced money transfers flowing through its providers' money transfer systems. In fact, historically, Walmart has been responsible for more complaints about fraud-induced money transfers than any other agent worldwide. For example, for MoneyGram, between January 1, 2013 and December 31, 2018, Walmart was responsible for approximately 56 percent of all complaints about fraud-induced money transfers through MoneyGram worldwide. For Ria, from 2015 through 2018, Walmart was responsible for between approximately 89 to 93 percent of all of the complaints about fraud-induced money transfers through Ria worldwide. For Western Union, between January 1, 2013 and December 31, 2018, Walmart was responsible for approximately 22 percent of all complaints about fraud-induced money transfers in Canada, where Walmart is one of its agents.

Walmart's Role in Detecting and Preventing Fraud

32. As an agent dealing directly with consumers who send and receive money transfers through one or more providers, Walmart is well positioned to detect and prevent fraud-induced transfers.

33. Walmart's role as a large agent offering multiple money transfer services makes it integral to that effort because Walmart controls whether to: implement and maintain policies and procedures concerning fraud-induced transfers, educate and train its employees on consumer fraud, supervise its employees to ensure they are complying with anti-fraud policies and procedures, provide fraud warnings to consumers, monitor and investigate money transfer activity to identify unusual or suspicious activity, and take actions to prevent consumers from

2009 Order enjoined violations of any provision of the TSR, as promulgated or later amended, by providing substantial assistance or support to any seller or telemarketer, and also enjoined MoneyGram and its agents from failing to establish, implement, and maintain a comprehensive anti-fraud program designed to protect U.S. and Canadian consumers from fraud-induced money transfers worldwide. The 2009 Order's requirements included, but were not limited to, providing warnings to consumers, providing appropriate and adequate ongoing education and training on consumer fraud at all locations, taking reasonable steps to monitor and investigate activity at locations to detect and prevent fraud, taking reasonable steps to identify locations that are involved or complicit in fraud, and routinely reviewing and analyzing data regarding money transfer activities that are unusual or suspicious. On February 1, 2010, Walmart acknowledged receipt of the 2009 Order. In several presentations made to FTC staff, beginning in or around April 2010, Walmart representatives committed to developing a plan to reduce fraud that would focus on associate training and consumer education. Walmart also represented that it had already implemented a comprehensive anti-fraud program.

36. 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 amendment became effective on June 13, 2016, and prohibits the use of such money transfers for goods or services offered or sold through telemarketing or charitable contributions solicited or sought through telemarketing.

37. In or around January 2017, Western Union and its agents, including Walmart, became subject to the Stipulated Order for Permanent Injunction and Final Judgment in *FTC v. Western Union*, No. 17-cv-0110 (M.D. Pa. Jan. 19, 2017) ("2017 Western Union Order"). Under that order, Western Union and its agents must establish, implement, and maintain a

comprehensive anti-fraud program designed to protect consumers worldwide by detecting and preventing fraud-induced money transfers. The Order's requirements also include, but are not limited to, providing warnings to consumers, appropriate and adequate education and training to front line employees, monitoring of activity to prevent fraud-induced money transfers, investigation of and disciplinary action against agents, and adequate systematic controls to detect and prevent fraud-induced money transfers. The Order also addresses compliance with the TSR Amendment's prohibition of cash-to-cash money transfers and requires Western Union and its agents to identify, prevent, and post cash-to-cash money transfers initiated or received in the U.S. from being used as a form of payment in telemarketing transactions. These requirements include asking consumers before they transfer money whether their transfers are to pay for goods or services offered or sold through telemarketing and declining to process such money transfers. Finally, the order mandates that Western Union and its agents warn consumers that it is illegal for any seller or telemarketer to accept money transfers as payment for goods or services sold through telemarketing. On January 27, 2017, Western Union provided Walmart with a copy of the 2017 Western Union Order.

38. In November 2018, a Stipulated Order for Compensatory Relief and Modified Order for Permanent Injunction ("Modified Order") was entered against MoneyGram. That Modified Order expanded the anti-fraud requirements of the 2009 Order to protect consumers worldwide and has similar requirements to the 2017 Western Union Order. It also required MoneyGram to pay $125 million in compensatory relief. On December 5, 2018, Walmart acknowledged receipt of that order.

39. Walmart's agreements with its providers require it to comply with any orders, judgments, or decrees that apply to its providers, as well as any applicable laws. As an MSB, Walmart 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.

40. Even in the face of these independent obligations to detect and prevent consumer fraud and money laundering, for many years, Walmart has failed to: (a) establish, implement, and maintain a comprehensive and effective anti-fraud program designed to detect and prevent consumer fraud; (b) properly train and ensure that its employees are knowledgeable about anti-fraud and AML policies and procedures designed to prevent consumer fraud; (c) adequately oversee and supervise employees responsible fo

scams, lottery or prize scams, imposter scams, cyber or malware scams. 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. In these scams, consumers often are instructed over the telephone, through text messages, by email, or over the Internet to send money transfers. The telemarketers and con artists use false or misleading statements to induce consumers either to pay for purported goods or services, such as loans or large cash awards, or to make payments as a result of purported circumstances, such as emergencies, that do not exist.

42. Victims of fraud-induced money transfers often send their money transfers from Walmart locations. In some cases, fraudsters even direct consumers to send their money transfers from a Walmart location. In many cases, older consumers (ages 65 and older) have been financially exploited by sending money transfers in connection with common telemarketing scams, such as grandparent scams, Good Samaritan scams, lottery or prize scams, and romance scams, from Walmart locations. The average loss suffered by older consumers is usually greater than for younger consumers. In addition, perpetrators of the scams, or those acting on their behalf, including fraud rings and money mules, frequently collect the proceeds of the frauds from Walmart locations, and in some instances, those individuals have even been employees of Walmart.

43. MoneyGram's, Ria's, and Western Union's records show that Walmart has been responsible for a substantial amount of fraud-induced money transfers through their money transfer systems. As Walmart is aware, many fraud-induced money transfers described in those records involve telemarketing scams. Between January 1, 2013 and December 31, 2018, Walmart locations were responsible for processing at least $197,316,611 in money transfers that were the subject of complaints and over $1.3 billion in money transfers that were related to those complaints and therefore could have been fraud-induced.

a. Information from MoneyGram indicates that between January 1, 2013 and December 31, 2018:

1) MoneyGram received a total of at least 176,672 complaints reporting losses of $159,594,760 (including fees) involving Walmart, including complaints about the following scams, which typically involve telemarketing:

a) at least 19,035 complaints with losses of $19,386,770 about person-in-need or grandparent scams;

b) at least 15,401 complaints with losses of $7,749,949 about advance fee, loan-grant, or other loan scams;

c) at least 10,192 complaints with losses of $7,844,700 about romance scams;

d) at least 8,375 complaints with losses of $5,879,474 about lottery scams;

e) at least 1,590 complaints with losses of $1,971,761 about IRS and utility scams, including investment scams involving IRS imposters; and

f) at least 355 complaints with losses of $351,857 about cyber, malware, or other tech support scams.

2) An additional 695,404 money transfers with total losses of $376,322,686 (including fees) were linked to complaints received by MoneyGram about fraud-induced money transfers involving Walmart.

3) Although Walmart has accounted for approximately 26 percent of MoneyGram's money transfers based on volume and approximately 24 percent based on dollar amount, Walmart was responsible for sending or paying out approximately 56 percent of all complained-about fraud-induced money transfers worldwide through MoneyGram.

b. Information from Ria indicates that between April 24, 2014 and December 31, 2018:

1) Ria received a total of at least 43,603 complaints reporting losses of $32,741,212.93 (including fees) that were sent from or received at a Walmart location, including complaints about the following scams, which typically involve telemarketing:

a) at least 4,815 complaints with losses of $2,525,065 about prize and lottery scams;

b) at least 3,092 complaints with losses of $1,809,725 about Good Samaritan scams;

c) at least 1,641 complaints with losses of $884,413 about romance and online dating scams;

d) at least 1,514 complaints with losses of $2,035,382 about emergency or grandparent scams;

e) at least 924 complaints with losses of $623,907 about advance-fee loan scams;

f) at least 855 complaints with losses of $565,062 about elder abuse scams;

g) at least 385 complaints with losses of $256,270 about debt relief scams; and

h) at least 54 complaints with losses of $62,532 about IRS imposter scams.

2) An additional 2,056,697 money transfers totaling $878,383,329.49 (without fees) were transactions conducted by senders or recipients of fraud-induced money transfers, and therefore, were potentially related to fraud.

3) Walmart has accounted for approximately 36 percent of Ria's money transfers based on volume and approximately 27 percent of Ria's money transfers based on dollar amount, but in 2017 alone, Walmart accounted for approximately 93 percent of Ria's fraud cases based on volume and approximately 89 percent of Ria fraud cases based on dollars. In 2018, Walmart accounted for approximately 87 percent of Ria's fraud cases based on volume and approximately 90 percent of Ria fraud cases based on dollars.

c. Information from Western Union indicates that between January 1, 2013 and December 31, 2018:

1) Western Union received a total of at least 6,404 complaints reporting losses of $4,980,638.36 (including fees) involving Walmart in Canada, including 1,889 complaints totaling $1,228,446 about transfers that originated from or were paid out in the United States.

45. In March 2017, at least 4,974 fraud-induced money transfers totaling $5,081,268.62 were reported to MoneyGram and Ria concerning transactions that were either sent from or paid out at a Walmart location, or both. These were the largest monthly totals of reported fraud-induced transfers since February and March 2016, when MoneyGram experienced technical problems with its interdiction system, as described below.

46. For many years, Walmart also has been aware of consumer fraud involving its stores, including particular locations that had very high levels of consumer fraud and suspicious activities. In fact, MoneyGram and Western Union have provided information to Walmart about certain locations in the United States and Canada that had fraud rates of more than 25 percent, 50 percent, or even 75 percent of their money transfer activity (based on the number or dollar amount of transactions) when taking into account confirmed fraud and linked or potential fraud. Although Ria did not provide Walmart with similar information about fraud rates at its locations based on confirmed and linked or potential fraud, it did provide Walmart with information about confirmed fraud at locations, as well as unusual or suspicious activity, such as transactions that had bad addresses, including addresses that were P.O. boxes, incomplete, or listed as "anywhere," "unknown," or "not given."

47. In May 2018, Walmart conducted an analysis of Walmart locations in the United States that would be classified as an Elevated Fraud Risk Agent Location ("EFRAL") under the 2017 Western Union Order, and determined that, from January 2017 through January 2018, there were 317 instances in which Walmart stores met the EFRAL criteria, including 12 stores that had 15 or more complaints in a two-month period. The remaining 305 stores had five or more complaints that amounted to five percent or more of money transfers received at those locations. Those 317 separate instances involved 190 unique Walmart store locations because some of the stores had met the criteria more than once.

Walmart has Failed to Effectively Detect and Prevent Fraud-Induced Money Transfers

48. For many years, perpetrators of frauds, including fraudulent telemarketers, sellers, and con artists, have accessed and exploited Walmart's money transfer services, and Walmart's locations have played an integral role in the scams. Walmart's locations have been more susceptible to fraud-induced money transfers in part due to the thousands of associates authorized to provide money transfer services at its locations, the high turnover rate of associates, heavy customer traffic, and/or various shifts of associates working at a single location. In addition, as a dual agent for MoneyGram and Ria in the United States, there is a heightened risk of consumer fraud at its locations because consumers can send and receive money transfers through two different money transfer companies without being detected by those companies. Walmart has been, or should have been, well aware of these facts.

49. Walmart nonetheless has failed to take basic and important steps to address consumer fraud, including by failing to implement and maintain effective policies and procedures to detect and prevent fraud, provide education and training that included clear directions to its employees about detecting and preventing consumer fraud, supervise and oversee its employees to ensure that they are complying with anti-fraud and AML policies and procedures, routinely provide fraud warnings to consumers, adequately monitor and investigate money transfer activity to determine if there is any unusual or suspicious activity, and take effective actions to prevent consumers from sending or receiving fraud-induced money transfers, including those related to telemarketing.

50. In many instances, Walmart's locations have not complied with Walmart's providers' anti-fraud or AML policies and procedures. Walmart also has not taken adequate and timely steps to address the deficiencies and inconsistencies in its own anti-fraud program, policies, and procedures and to address consumer fraud at its locations. In addition, in some

cases, Walmart has had corrupt or complicit employees at its locations that have facilitated the payments of fraud-induced money transfers. As a result of Walmart's failure to implement and maintain a comprehensive anti-fraud program to detect and prevent consumer fraud, it has played a significant role in sending and receiving fraud-induced money transfers through its providers' money transfer systems. These failures have caused many millions of dollars in consumer losses, without providing benefits to consumer competition that has outweighed the harm suffered by defrauded consumers.

Walmart has Failed to have a Comprehensive Anti-Fraud Program

51. For many years, Walmart has failed to establish, implement, and maintain its own comprehensive anti-fraud program, policies, procedures, and controls designed to detect and prevent consumer fraud even though Walmart has been aware that there was a substantial amount of fraud-induced money transfers moving through the money transfer systems at Walmart's locations. Until in or around November 2014, Walmart did not even have a written anti-fraud and consumer protection program documenting its policies and procedures for detecting and preventing consumer fraud at its locations.

52. Even after establishing a written anti-fraud program, in some cases, Walmart violated its own program requirements. For example, although Walmart's anti-fraud program required stores that had been identified by its providers as having higher incidents of fraud received at their locations to complete "Receive Fraud Training" within seven days of when the training was assigned, in many cases, those locations did not comply with that requirement. In some cases, the training required by MoneyGram at particular locations was not completed for months after Walmart's policies required it. In addition, even though Walmart's anti-fraud program required Walmart stores to have certain consumer education and awareness materials,

including consumer fraud warnings and pamphlets, in many cases, Walmart locations have not complied with those requirements.

53. For many years, Walmart's anti-fraud program also had no written procedures for its associates to prevent suspected or known fraud-induced money transfers from being paid out at its locations. For example, in Walmart's July 2014 and November 2017 programs, although there were written procedures on how Walmart associates should respond when they suspected that senders of money transfers may be victims of fraud, there were no written procedures for how Walmart associates should respond when they suspected that receivers of money transfers may be potential fraudsters.

54. On April 19, 2017, MoneyGram conducted a Home Office Review of Walmart's anti-fraud program and found that: (1) Walmart had not effectively prevented fraud transactions; (2) Walmart had not properly completed required information on transaction records; and (3) Walmart had not reported, filed, or referred Suspicious Activity Reports ("SARs") as required. In an August 10, 2017 letter to Walmart, MoneyGram explained that the main concern for the finding that Walmart had not effectively prevented fraud transactions was because, "at the policy level," Walmart was "not rejecting potential consumer fraud related transactions on the receive end."

Walmart's Deficient Practices Related to Receive-Side Fraud

55. According to Walmart's written anti-fraud program, Walmart's goal was "to educate, detect, investigate, respond, and deter consumer fraud against our customers." Despite that stated goal, Walmart failed to implement practices designed to effectively detect and prevent fraud-induced money transfers received at its stores, and instead assisted and facilitated fraud by adopting practices that were harmful to consumers. For example, in 2015, Walmart adopted a practice of not training its employees to deny or reject payouts to suspected fraudsters at the

point of sale. Although Walmart trained its employees to refuse to send money transfers if they believed the sender was a victim of fraud (referred to as "send-side fraud"), it did not direct its employees to deny or reject payouts to receivers of suspected fraud-induced money transfers (referred to as "receive-side fraud"). Instead, Walmart's training instructed employees not to deny those transfers, but instead to report them by faxing a paper Money Services Activity Report ("MSAR") to Walmart's Home Office. In May 2017, Walmart replaced this paper MSAR system with an Electronic Money Services Activity Report ("eMSAR"), as described below. In addition, the Quick Reference Guide for employees that was in use from in or around November 2016 until sometime in 2018, stated, "If you suspect fraud, complete the transaction," and report it to MoneyGram and Walmart's Home Office. Walmart adopted this practice despite knowing that once the money transfers were paid to suspected fraudsters, fraud victims typically could not get their money back. Walmart continued this practice despite being told by MoneyGram, after MoneyGram learned about this practice in 2015, that it expected Walmart and its employees not to pay out money transfers to suspected fraudsters.

56. By failing to have consistent policies, procedures, and practices requiring its employees at its stores to deny and not pay money transfers to suspected fraudsters, Walmart's locations were more susceptible to consumer fraud, thereby substantially assisting fraudsters, including telemarketers and sellers, and causing significant financial injury to victims of fraud-induced money transfers. From September 2015 through October 2018 and again from December 2018 through May 2019, Walmart's receive-side fraud rate by volume for domestic transfers through MoneyGram was higher than the rates for the rest of MoneyGram's agent network in the United States. In March 2017 alone, Walmart's fraud rate for receive-side fraud based on the dollar value was approximately three-and-four times higher than the rest of MoneyGram's U.S. agents.

57. Walmart did not begin to adjust its practice of not training its employees to reject suspected receive-side fraud transactions at the point of sale until May 2017—after MoneyGram began suspending Walmart locations for the first time. Even then, this remedial training was only provided to some Walmart employees at problematic locations that MoneyGram required to have additional training because the locations had been suspended or identified as having higher incidents of consumer fraud.

58. Walmart's remedial training included instructions about the company's new eMSAR process for canceling and reporting transactions to Walmart's Home Office, which did not effectively address Walmart's handling of receive-side fraud. For example, from May through at least October 2017, Walmart's remedial training instructed associates to reject certain suspected receive-side fraud transactions at the point of sale by using the "Scam" option in eMSAR—but the eMSAR menu interface contradicted this, stating instead that the option was to be used *only* for fraud against Walmart customers who may be victims of a scam or against Walmart itself, rather than for potential fraudsters. In addition, although there was an option in eMSAR for "Suspicious Behavior During a Money Transfer Receive," the eMSAR menu indicated that associates should only use that option when the customer had received *more than* five different transactions in a single day—five fraud-induced money transfers per day would not qualify. And even worse, the direction in eMSAR was only to report, but not to cancel, those transactions.

59. In or around November 2017, Walmart finally changed its remedial training, as well as its eMSAR menu, to instruct associates to use the "Suspicious Behavior During a Money Transfer Receive" to cancel certain suspicious transactions on the receive side at the point of sale. However, Walmart still directed its associates to use that option only in two very limited circumstances: (1) when a customer had multiple high-dollar amount receives during the same

day or multiple times a week, or (2) when a customer presented different IDs during different visits, such as IDs with different names. The only other eMSAR option that could apply to suspected receive-side fraud, "Conversation (Customer said something suspicious to you or another customer)," only instructed employees to report the transaction to Walmart's Home Office, but did not instruct them to cancel it.

60. From May 2017 until late 2018, regardless of whether associates used the "Scam" or "Suspicious Behavior During a Money Transfer Receive" option to cancel transactions, those eMSAR options only reported the transactions to Walmart's Home Office. That meant suspected fraudsters could go to another Walmart employee or to a different location to pick up their transfers, because information about those consumers and their cancelled transactions were not necessarily reported to MoneyGram or Ria in a timely fashion. Although Walmart's remedial training at this point also instructed associates to call the provider (MoneyGram or Ria) to report their suspicions after the customer left, so that the provider could systematically block the transfer from being picked up elsewhere, Walmart associates often failed to do so.

61. In addition, Walmart's regular annual training and resource materials for employees in Walmart's Customer Service Desks and MoneyCenters gave contradictory guidance regarding the handling of receive-side fraud—they continued to direct employees not to deny and to "complete" the suspected fraud transactions, and only then to report them as suspicious. Walmart's annual training for salaried managers also provided more limited content on consumer fraud overall and only focused on refusing to send, but not refusing to pay out, potential fraud-induced money transfers.

62. Walmart did not update its annual training to instruct associates that if they "have identified a potential fraudster," they should refuse the transaction and report it using the eMSAR process until at least late 2018. Even then, however, Walmart still gave its associates

mixed signals, telling them elsewhere in the training that they should not deny a suspicious transaction when a customer has received "large dollar amounts, multiple times a day," and he "appears nervous and has gone to different registers each time." Because this was an annual training, moreover, many Walmart associates did not have to complete this training until sometime in 2019.

63. Although the updated annual training for both associates and supervisors instructed that "managers and supervisors should not override your decision to reject a financial service transaction when you suspect that the customer may be a victim of a fraud or scam," it did not provide the same instruction for a payout to a potential fraudster. The updated annual training for salaried managers also continued to focus only on refusing the transactions of customers who may be victims of fraud. Therefore, this updated annual training continued to provide inconsistent instructions for employees regarding the handling of suspected receive-side fraud.

64. It was only in late 2018 that Walmart's eMSAR process became automated so that it could transmit information directly to Walmart's providers without Walmart associates having to make a phone call to the provider to report suspected disasters. Despite that, in many cases, the eMSAR process for preventing payout of fraud-induced money transfers and training has continued to be ineffective because (1) Walmart's annual training has provided inconsistent instructions on the handling of suspected receive-side fraud; (2) as described more fully below, Walmart has failed to ensure that its employees are properly trained and knowledgeable about the use of Walmart's eMSAR process for stopping suspected receive-side fraud; (3) Walmart's eMSAR menu options relating to receive-side fraud continue to be too limited, and include only such circumstances as multiple high-dollar money transfers received during the same day or over multiple weeks, or customers presenting different IDs during different visits; and (4) managers at Walmart locations have sometimes overridden associates' decisions not to complete transfers

even when associates have detected unusual or suspicious activity. As of at least August 2018, Walmart also had not implemented the eMSAR process at its locations in Mexico even though it was known to be one of the top five destinations for international fraud-induced money transfers.

65. For many years, despite Walmart's awareness that its locations have been used by known and suspected fraudsters to receive funds for scams, many of which have been executed through telemarketing, Walmart did not routinely train or instruct its associates to ask consumers receiving suspicious money transfers questions about the nature or purpose of their money transfers. Since the TSR Amendment went into effect in June 2016, Walmart also has not trained or instructed its associates to ask questions about whether consumers are receiving funds as payments for goods or services sold over the phone or for charitable contributions solicited or sought over the phone.

Walmart's Deficient Practices Related to Send-Side Fraud

66. Walmart also has failed for many years to effectively prevent consumers from sending fraud-induced money transfers, including those related to fraudulent telemarketing sales and illegal telemarketing payments, from Walmart locations. Despite Walmart's awareness that its locations were often used to send fraud-induced money transfers, for years, Walmart failed to provide clear and consistent instructions to its associates in its annual anti-fraud remedial training, as well as in some of its resource materials, about the necessary steps to effectively report and stop those transfers. As a result of Walmart's lax practices, in many cases, it has failed to prevent senders of fraud-induced money transfers, particularly the elderly, who are frequently defrauded through telemarketing schemes, from being victimized in a variety of scams, including, but not limited to, grandparent scams, Good Samaritan scams, lottery or prize scams, and romance scams. In some cases, fraudsters have directed consumers to send their money transfers from Walmart locations due to Walmart's lack of safeguards.

67. In many cases, Walmart has failed to take adequate measures to prevent consumers from sending money transfers that have characteristics indicative of fraud, such as multiple money transfers in relatively short periods of time, transfers to high-risk countries known for fraud, transfers in amounts that far exceed the average money transfer, and transfers to different individuals. For example, from February to March 2017, Walmart sent 52 transfers totaling $51,000 for one potential victim of elder financial exploitation to seven different receivers in Ghana and the United States. Similarly, in March to April 2017, Walmart sent 33 transfers totaling $54,550 for another such victim to a recipient in Ghana. Only after these numerous suspicious transfers and huge dollar losses were these matters finally referred to law enforcement and Walmart's providers. From May to July 2017, moreover, Walmart sent 42 transfers totaling $71,235.16 for another customer to different receivers in Ghana, the United States, and Turkey before Walmart finally referred the matter to law enforcement and the provider after receiving multiple referrals from Walmart associates. According to one referral from a Walmart associate, the customer indicated he was sending the money to buy millions of dollars in gold.

68. In many cases, Walmart locations have also not provided required warnings to senders about common money transfer frauds sent or received through its stores. For example, even though FTC orders have required Walmart to use send forms that include a consumer fraud warning on the front page, in some cases, Walmart stores were missing the required send forms, or have used send forms that omitted the required consumer fraud warnings. In other cases, Walmart stores have not displayed consumer fraud warning signs or had consumer fraud brochures or pamphlets available. For example, in a presentation provided to Walmart in October 2019, Ria expressed concern that 39 percent of the Walmart stores it visited between

January and August 2019 were missing fraud awareness materials, and it also noted that 24 percent of the stores were missing send forms.

69. Signs and send-form warnings alone are not enough, however, because consumers are not generally aware of the risks associated with money transfers, including the possibility that recipients can use false information or fake IDs to pick up money transfers. Despite being well aaware of these risks, Walmart for years failed to take adequate steps to address them. Until at least March 2019, Walmart did not even take steps to ensure that its associates asked senders questions about whether their transfers were related to telemarketing or warned them about the fact that the TSR prohibits cash-to-cash money transfers as a form of payment for telemarketing transactions.

Walmart has Failed to Properly Train its Employees about Anti-Fraud and AML Policies and Procedures

70. Walmart and its providers have historically recognized that employees responsible for processing money transfers are the first line of defense in detecting and preventing consumer fraud, and Walmart's providers have relied on Walmart to train its own employees in the policies and procedures required for detecting and preventing fraud. Although Walmart has long been aware of the importance of training employees responsible for providing or supervising money transfer services, it has failed to ensure that its employees are properly trained and are sufficiently knowledgeable about anti-fraud and AML policies and procedures. These employees may perform up to hundreds of thousands of dollars in financial transactions for consumers during a single shift. On numerous occasions, Walmart also has failed to promptly provide mandatory consumer fraud training as a remedial action for all employees at its high or higher fraud locations identified by its providers. For years, although MoneyGram

required Walmart to provide remedial training to employees at high-fraud locations, Walmart failed to ensure that all employees at those locations had promptly received the required training.

71. Walmart's written policy, as well as Walmart's contractual obligations with its providers, recognize the importance of training and require that all Walmart employees responsible for providing money transfer services receive initial and ongoing training. Walmart has primarily provided this training through annual computer-based learning. For many years, however, Walmart has failed to ensure that its employees responsible for providing money transfer services have taken the required training, are up to date on their training, or taken relevant training before providing money transfer services. For example, until at least September 2015, Walmart did not even begin providing required training for the tens of thousands of secondary employees, who fill in for the primary employees responsible for providing money transfer services. Moreover, Walmart's Home Office did not have the ability to assign all of the relevant training relating to providing money transfer services to its secondary employees at Walmart locations until sometime in mid to late 2018.

72. For many years, Walmart's annual training for associates, supervisors, and managers with responsibilities for providing money transfer services have included limited information about detecting and preventing consumer fraud involving money transfers. For example, Walmart's annual training, which takes between 20 to 45 minutes to complete, has primarily covered AML topics, while providing only limited directions on the handling of suspected fraud-induced money transfers. As described above, for many years, Walmart's annual trainings did not even direct its associates to reject paying out money transfers if they suspected that the customers were fraudsters. In addition, Walmart's trainings for its managers provided very little information about detecting and preventing fraud-induced money transfers.

73. Despite receiving advance notice from its providers that they were going to be conducting compliance reviews or audits of their Walmart locations, for many years, the providers have found that Walmart's employees lack the proper training and knowledge about anti-fraud and AML policies and procedures relating to money transfers, including with respect to detecting and preventing fraud, accurately recording customers' biographical information and IDs, and reporting, stopping, or otherwise addressing suspicious activities at those locations.

74. A 2014 audit conducted by MoneyGram found that numerous Walmart locations had untrained or undertrained employees providing or supervising money transfer services in Walmart's Customer Service Desks and MoneyCenters. MoneyGram informed Walmart that an audit of 397 Walmart locations disclosed that 1,863 "primary and secondary" employees responsible for processing money transfers had not had either initial or ongoing training, and 68 percent of them were secondary employees who had never taken the required training. Walmart's internal documents indicate that MoneyGram's 2014 audit found that overall, 39 percent of Walmart locations had untrained primary employees and 60 percent had untrained secondary employees.

75. Even after Walmart implemented a new audit preparation protocol in early 2015, which involved corporate communications, conference calls, and webinars with the stores in advance of audits, Walmart still continued to have untrained or undertrained employees who provided, or supervised the provision of, money transfer services. For example, in March 2015, MoneyGram identified a Walmart store in Houston, Texas as having the largest number of untrained employees ever found in a MoneyGram audit. By May 2015, Walmart was aware that at least 15 percent of its stores continued to have untrained or undertrained employees working in, or supervising, money transfer services. Moreover, between January 2015 and July 2016, MoneyGram's review of 323 Walmart locations across the country revealed that 61 (or

approximately 19 percent) of them had employees who had not completed either initial or ongoing compliance-related training. Similarly, from July through September 2017, MoneyGram's reviews of 87 stores in 14 states revealed that 30 stores (or 34 percent) had employees who had not completed ongoing compliance-related training. Ria's reviews of stores resulted in similar findings. For example, in September and October 2018, Ria's reviews of 95 stores revealed that Walmart had at least 600 associates at those locations who were past due on training.

76. Although Walmart recognized the need to implement point-of-sale register lockouts as a control to prevent employees who were not properly trained or knowledgeable about anti-fraud and AML procedures from processing money transfers, it took several years—until at least in or around mid to late 2018—for Walmart to finally implement the lockouts. However, even with the lockouts, Walmart's providers have continued to find locations that had untrained, undertrained, or unknowledgeable employees providing money transfer services. For example, in July 2019, Ria's reviews of 48 Walmart locations in four states continued to uncover associates with incomplete training and insufficient knowledge on a variety of anti-fraud and AML topics and procedures. Three of those stores had unsatisfactory reviews, including two stores with repeat unsatisfactory reviews, and findings included employees with little or no training, poor knowledge about anti-fraud and AML requirements (including Walmart's eMSAR process), and associates even sharing User Operator ID numbers and passwords—a tactic Walmart's providers prohibit because it allows unauthorized users to access their money transfer systems.

77. In addition to failing to conduct the required initial and ongoing training for employees, in many cases, Walmart also failed to provide prompt mandatory training when necessary for its employees. The 2009 Order required, among other things, that MoneyGram

and its agents take "[p]rompt disciplinary action…, including [by] requiring mandatory fraud training" against any location or person authorized to sell money transfer services to prevent fraud-induced money transfers. Despite that requirement, in many cases, Walmart has not promptly trained its employees when MoneyGram identified particular locations that had high levels of fraud and required such training. For example, in some cases, Walmart has failed to conduct prompt consumer fraud training and has had locations with outstanding mandatory trainings of more than 30, 60, or even 90 days. For the reasons explained above, Walmart's remedial fraud training also has been deficient in many respects.

78. For many years, the training and resource materials used by Walmart to educate its employees about anti-fraud policies and procedures also have been deficient. For example, as explained above, while Walmart's training typically directed employees to refuse to send money transfers when they identified red flags indicating a sender may be a victim of fraud, until at least mid to late 2018, that training directed employees only to complete paper MSARs, but not to refuse payouts, when they identified red flags indicating a receiver may be a suspected fraudster. For many years, Walmart's resource materials also only focused on preventing fraud when employees suspected customers were the victims of fraud, not the perpetrators. A Walmart Quick Reference Guide even directed employees to complete transactions when they identified red flags indicating that customers may be receiving funds because they are committing consumer fraud.

79. Even though Walmart has been aware for many years that consumers often use fake IDs when receiving fraud-induced money transfers, for years, Walmart has provided inadequate training and resource materials to its employees on identifying and preventing the use of fake IDs at its locations.

80. For years, Walmart has failed to provide

its employees, assign employees authorized to process money transfers with unique User or Operator ID numbers and passwords for their individual use, give employees resource materials containing information about policies and procedures relating to money transfer services, ensure that its employees are complying with all policies and procedures, and monitor the activities involving its Customer Service Desks and MoneyCenters to ensure compliance with all anti-fraud and AML policies and procedures. Indeed, Walmart's providers require Walmart to perform these oversight responsibilities.

82. Walmart's oversight of its employees at its Customer Service Desks and in its MoneyCenters is especially important because of the large number of employees responsible for providing money transfer services and the high volume of money transfers conducted at Walmart's locations. For example, in 2014, Walmart had approximately 2.2 million employees worldwide, of which approximately 1.3 million were based in th

January through August 2019, Ria's reviews of 473 stores revealed that 188 stores were considered "critical h8e

contained in the MSB Binder. In addition, as described below, for many years, Walmart's providers have found that some Walmart stores did not have the required send forms (with consumer fraud warnings), fraud awareness brochures or pamphlets, or consumer fraud warning signs.

86. For many years, both MoneyGram's and Ria's compliance reviews of Walmart locations have also found that Walmart's employees have not been complying with the providers' and/or Walmart's policies and procedures for providing money transfer services. For example, in 2015 and 2016, MoneyGram's compliance reviews of hundreds of Walmart locations routinely found that Walmart's employees had failed to properly complete required information for transaction records, report or escalate suspicious activities as required, and verify customers' identities when required. In 2017, MoneyGram informed Walmart that throughout its monthly reviews of locations, it had repeatedly found that Walmart locations were not properly completing required information in transaction records, and that "[c]apturing incomplete or incorrect data directly not only impacts MoneyGram's capacity to monitor and interdict customers efficiently, but it also affects Wal-Mart since it keeps bringing suspicious customers to Wal-Mart locations." For example, during MoneyGram's monthly call with Walmart on July 6, 2017, MoneyGram included information about its QA reviews of 29 stores and highlighted that at least five of those stores had significant data integrity issues for money transfers sent from those stores. In fact, no physical address or an incomplete address (with no street name or house number) had been recorded for between 9 and 28 percent of all money transfers sent from those locations.

87. In addition, although Walmart's employees

stores in 14 states revealed that 64 percent of the locations were not knowledgeable about eMSARs or were not escalating or referring eMSARs as required. In January 2018, a MoneyGram audit of 24 stores in Florida and Texas, which had over 50,000 money transfers sent and over 19,000 money transfers received in each month period, revealed that: (1) 25 percent of the stores were not executing eMSARs—which meant they were not stopping fraud at the location; (2) 58 percent of the stores were executing eMSARs, but were not calling MoneyGram to ensure that the consumers' money transfers were stopped; (3) 33 percent of the stores had secondary associates who were authorized to provide money transfer services, but were not experienced or knowledgeable about how to execute eMSARs; and (4) 46 percent of the stores had associates who were identified as needing to be removed from their roles in financial services.

88. MoneyGram's reviews in 2018 and 2019 continued to find that Walmart associates lacked knowledge about the eMSAR process, as well as other basic and important procedures. For example, from April to July 2018, MoneyGram's reviews of 1,586 associates at 219 stores in 16 states, the District of Columbia, and Puerto Rico found that between 404 and 1,019 associates needed training on suspicious activity, fraud examples, eMSAR usage, and ID acceptance. From March to May 2019, MoneyGram's reviews of 155 stores in 16 states and the District of Columbia found that hundreds of associates needed training about ID requirements and acceptance, and eMSAR usage and knowledge. Moreover, for 2019 overall, MoneyGram's reviews of 476 stores in numerous states found that at least 40 percent of associates needed training on potentially suspicious activity, 36 percent of associates needed training about eMSAR knowledge, and 18 percent of associates needed training on ID acceptance and requirements.

89. Ria's reviews of Walmart stores made findings similar to those in MoneyGram's reviews. For example, from January through August 2019, Ria's reviews of 473 Walmart stores in 30 states found that a substantial number of Walmart associates—between 414 and 1,400—needed training about eMSAR usage and knowledge of fraud, suspicious activity, ID requirements and acceptance, structuring (breaking up transactions into smaller dollar amounts) and flipping (shortly after receiving funds, sending a large portion to another recipient).

90. Walmart's failure to properly supervise and monitor employees at its Customer Service Desks and MoneyCenters has also allowed employees to become complicit in the frauds. Walmart's internal records show numerous instances in which employees have been complicit, or possibly complicit, in the frauds. These records demonstrate that, for many years, employees have, among other things, received cash tips for their assistance in processing fraud-induced money transfers, allowed individuals to use multiple names and/or IDs in picking up money transfers, used the same personally identifiable information for different customers, structured transfers for customers to avoid ID requirements, made up fictitious information for customers, or conducted suspicious money transfers themselves. For example, in 2013, a Customer Service Department associate engaged in flipping, where she received money transfers from multiple senders in the United States, kept a portion for herself, and sent a portion of the funds to receivers in other countries. She also had other associates facilitate her activity by going to different coworkers in her department in order to try to avoid detection. In 2014, a MoneyCenter associate admitted she had received several hundred dollars on multiple occasions from customers using different names and performing fraudulent transactions. In 2015, a different MoneyCenter associate, who was the subject of three complaints received by MoneyGram in 2014, received at least 12 transfers totaling $613.35 and sent at least 32 transfers totaling $32,059 to Nigeria and Ghana in approximately a two and a half months. In 2016 and early 2017,

and high turnover of associates responsible for processing money transfers; heavy customer traffic at its MoneyCenters and Customer Service Desks; deficiencies in Walmart's anti-fraud program, including with respect to the training, knowledge, and oversight of its associates responsible for providing money transfer services; and Walmart's dual agency in offering money transfers through two money transfer systems.

94. Walmart has primarily relied on its providers to block certain money transfer activity, including money transfers of individuals who have been the subject of complaints, even though Walmart has been aware of weaknesses and deficiencies in its providers' interdiction (blocking) systems that make those systems susceptible to use by fraudsters, as well as the inherent risks that come with having more than one provider. For example, Walmart has been aware that these interdiction systems can be circumvented by consumers simply by changing certain pieces of biographical information, such as names, addresses, or dates of birth, or by using fake IDs or switching to another money transfer provider at Walmart. In addition, from approximately April 2015 through October 2016, MoneyGram experienced some technical problems with its interdiction system, which is used to block consumers, including suspected fraudsters, in its network. Walmart did not become aware of MoneyGram's interdiction system difficulties until mid-2016, even though Walmart's own monitoring of money transfers should have alerted it sooner that MoneyGram was not properly blocking suspected fraudsters and repeat victims. Because Walmart relied on its providers' blocking systems, instead of having its own, and its practice was not to train its employees to reject payouts of money transfers that were suspicious and potentially fraudulent, Walmart's failures on these fronts made fraud-induced money transfers through its stores more likely.

95. Walmart has had inadequate and ineffective policies and procedures for submitting information to its providers and requesting that certain consumers be blocked from

sending or receiving money transfers due to their suspicious money transfer activity. Walmart did not even begin providing Ria with lists of consumers to be blocked in its network until mid to late 2016. In addition, for years, when employees faxed MSARs or submitted eMSARs regarding potential victims or suspected fraudsters to Walmart's Home Office, Walmart did not promptly submit requests to its providers that those individuals be blocked from using their money transfer systems. Walmart also has not provided the third-party responsible for preparing Walmart's blocking requests with the resources, such as consumer fraud reports and transaction data provided by Walmart's providers, to enable them to identify customers who should be blocked. In addition, for many years, when it identified customers with suspicious activity in one of its provider's systems, it only sent blocking requests to that provider, even though the customers could use other money transfer systems available at Walmart locations. Up until late 2018, Walmart also did not have any mechanism in place to ensure that when associates at its Customer Service Desks and MoneyCenters rejected a transfer at the point of sale, that information was promptly transmitted to Walmart's providers to prevent customers from going to another employee or location to send or receive their transfers.

96. Walmart also failed to adequately monitor suspicious money transfer activity at its locations, such as consumers receiving money transfers at multiple different Walmart locations in the same geographic area or visiting Walmart locations in different states. Instead, for many years, Walmart has primarily relied on its providers for addressing those suspicious activities, including for purposes of restricting or suspending Walmart locations, while failing to adequately address consumer fraud at its locations. In many cases, Walmart has not prevented consumers, including its own employees, from sending or receiving highly suspicious money transfers that it knew or had reason to believe were related to consumer frauds. In other cases, Walmart has continued to proce

suspicious characteristics or other indicators that the transfers were induced by fraud. For years, Walmart has frequently processed transactions that had suspicious characteristics, including: (1) high-dollar money transfers; (2) patterned activity, such as multiple transfers involving similar dollar amounts; (3) one-to-many or many-to-one transactional activity; (4) high-frequency money transfers; (5) transactions with data integrity issues (issues relating to ID numbers, addresses, dates of birth, or other information about recipients); (6) same IDs or addresses used by multiple receivers; (7) money transfers picked up using fake out-of-state IDs; (8) flipping; (9) structuring of transactions; (10) back-to-back transfers; (11) substantial transfers to high-risk countries known for fraud; (12) transactions where the sender and receiver do not appear to have a relationship; and (13) transactions with indications of elder financial exploitation due to the senders' age.

97. Based on information contained in MoneyGram's complaint database, fraud-induced money transfers at Walmart often have involved high-dollar amounts and have been picked up using out-of-state, including fake, IDs. From 2013 to 2018, money transfers of $900 or more accounted for over 47 percent of the total number of complaints involving Walmart. Of the reported fraud transfers paid at Walmart where the receiver's ID information was recorded, a majority (over 53 percent) of the transfers of $900 or more were picked up using an out-of-state ID.

98. Between January 2015 and February 2019, at least 101 Walmart locations have been responsible for paying out over $100,000 in fraud-induced money transfers that were the subjects of complaints, including at least 11 locations that paid out over $200,000 in transfers that were the subject of complaints. These locations include the following:

a. Walmart location #3159 in Teterboro, New Jersey paid out at least 150 reported fraud-induced money transfers totaling $272,945.50. Of the 101

Walmart locations responsible for paying out over $100,000 in reported fraud-induced transfers, this location had the highest average reported fraud amount at $1,819.64. This location paid out 63 reported fraud-induced transfers totaling $111,480.79 through MoneyGram and 87 reported fraud-induced transfers totaling $161,464.71 through Ria. A majority of the total complaints (72.6 percent) involved the grandparent or emergency scam. From May 9, 2017 until July 27, 2017, the location paid out 34 reported fraud-induced transfers through MoneyGram totaling $73,923.17, of which 88.2 percent (or 30 of the 34 transfers) involved receivers using an out-of-state ID to pick up the transfer. Over a two-year period, from September 24, 2016 to September 24, 2018, 93 percent of the Ria reported fraud-induced transfers paid by the location involved a phone call to the victim, and 85 percent involved the grandparent or emergency scam. MoneyGram and Ria have restricted receives at this location at least three times, including two restrictions by MoneyGram, from July to December 2017 and April to July 2018, and a more recent restriction by Ria, from October 2019 to January 2020.

b. Walmart location #5293 in Valley Stream, New York paid out at least 358 reported fraud-induced money transfers totaling $424,213.81. This location had the highest reported fraud by amount in the Walmart chain, of which, 141 fraud-induced transfers totaling $198,389.11 involved MoneyGram, and 217 fraud-induced transfers totaling $225,824.70 involved Ria. In 2017 alone, the location paid out 156 complaints totaling $214,455.80, of which 113 complaints totaling $136,546.68 were through Ria's system. MoneyGram and Ria have restricted receives atc 041laii2

from November 2018 to August 2019, and three restrictions by Ria, from January to March 2018, from August 2019 to January 2020, and more recently, in February 2020.

c. Walmart location #4383 in Dearborn, Michigan paid out at least 799 reported fraud-induced money transfers totaling $277,601.06, which was the largest volume of complaints in the Walmart chain. The location has paid out at least 322 fraud-induced transfers totaling $111,861.72 through MoneyGram and 477 fraud-induced transfers totaling $165,739.34 with Ria. Together, MoneyGram and Ria have disciplined this location at least nine times. MoneyGram has disciplined this location at least five times, including two restrictions on receives that were imposed in October 2015 and January 2017, and three suspensions, including two short suspensions in December 2017 and December 2018, and a thirteen-month suspension that began in January 2019. Ria has disciplined this agent at least four times, including at least three suspensions on receives, consisting of a four-month suspension in November 2017, a week-and-a-half suspension in December 2018, and a thirteen-month suspension beginning in January 2019, as well as at least one restriction on receives for a two-month period beginning in March 2018.

d. Walmart location #5129 in Landover Hills, Maryland has paid out at least 368 reported fraud-induced money transfers totaling $233,897.28, of which 162 reported fraud-induced transfers totaling $123,134.28 went through MoneyGram and 206 reported fraud-induced transfers totaling $110,763 involved Ria. MoneyGram and Ria have taken disciplinary actions against this location at least six times. MoneyGram restricted receives at this location at least twice, in

November 2015 and October 2016, and imposed a ten-day suspension in January 2019. Ria restricted receives at this location at least twice, from February to April 2018 and July to December 2019, and suspended receives at this location at least once, from January to February 2019.

Walmart has Failed to Adequately Warn Co

Walmart stores in 30 states and found that 114 stores (24 percent) of those stores did not have send forms and 186 stores (39 percent) of them were missing fraud awareness materials.

101. Like Ria, MoneyGram also routinely found that some of Walmart's stores were missing required materials relating to consumer fraud warnings. For example, in MoneyGram's April 2018 reviews of 47 stores in five states, MoneyGram found that four stores (nine percent) were missing send forms, five stores (11 percent) were missing fraud signs, and nine stores (19 percent) were missing fraud pamphlets. From April to July 2018, MoneyGram's reviews of 219 stores in 16 states, the District of Columbia, and Puerto Rico found that 18 stores (eight percent) were missing the consumer compla

112. Defendant and its employees have pr

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).

117. 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).

118. Section 5(m)(1)(A) of the FTC Act, 15 U.S.C. § 45(m)(1)(A), as modified by Section 4 of the Federal Civil Penalties Inflation Adjustment Act of 1990, 28 U.S.C. § 2461, as amended, and Section 1.98(d) of the FTC's Rules of Practice, 16 C.F.R. § 1.98(d) (2021), authorizes the Court to award monetary civil penalties of up to $46,517 for each violation of the TSR committed with actual knowledge or knowledge fairly implied. The Defendant's TSR violations were committed with the knowledge required by Section 5(m)(1)(A) of the FTC Act, 15 U.S.C. § 45(m)(1)(A).

COUNT II

Assisting and Facilitating TSR Violations

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

a. Induced consumers to pay for goods or services or charitable contributions through the use of false or misleading statements in violation of Section 310.3(a)(4) of the TSR, 16 C.F.R. § 310.3(a)(4);

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, 16 C.F.R. § 310.4(a)(4); and

c. Accepted cash-to-cash money transfers as payments for goods or services offered or sold through telemarketing or for charitable contributions solicited or sought through telemarketing in violation of Section 310.4(a)(10) of the TSR, 16 C.F.R. § 310.4(a)(10).

120. Therefore, Defendant's acts or practices, as set forth in Paragraph 119 violate the TSR, 16 C.F.R. §310.3(b).

CONSUMER INJURY

110. ioncumersare suffe andwill (coninute o sT)54 (uS)1.2 offe substa

and the TSR. Absmentinjunactve reliefe

D. Award any additional relief as the Court determines to be just and proper.

Dated: June 28, 2022

Respectfully Submitted,

/s/ Karen D. Dodge

KAREN D. DODGE
PURBAMUKERJEE
MATTHEW G. SCHILTZ
Attorneys for Plaintiff
Federal Trade Commission
230 South Dearborn Street, Suite 3030
Chicago, Illinois 60604
(312) 960-5634 (telephone)
(312) 960-5600 (facsimile)