

1 Taras Kick (Cal. Bar No. 143379)
taras@kicklawfirm.com
2 Tyler Dosaj (Cal. Bar No. 306938)
tyler@kicklawfirm.com
3 **THE KICK LAW FIRM, APC**
4 815 Moraga Drive
Los Angeles, CA 90049
5 Tel: (310)395-2988 / Fax: (310)395-2088

6 Daniel H. Charest (*pro hac vice* to be filed)
dcharest@burnscharest.com
7 Darren Nicholson (*pro hac vice* to be filed)
dnicholson@burnscharest.com
8 Chase Hilton (*pro hac vice* to be filed)
chilton@burnscharest.com
9 **BURNS CHAREST, LLP**
10 900 Jackson Street, Suite 500
11 Dallas, TX 75202
12 Tele: (469)904-4550 / Fax: (469)444-5002

13 **UNITED STATES DISTRICT COURT**
CENTRAL DISTRICT OF CALIFORNIA

14 JOSE GUZMAN, FORTINO RUTILO
15 JIMENEZ, AND BERTHA MEZA,
16 individually and on behalf of all others
similarly situated,

17 Plaintiffs,

18 v.

19
20 THE WESTERN UNION COMPANY, d/b/a
21 WESTERN UNION FINANCIAL SERVICES
22 INC., MONEYGRAM INTERNATIONAL,
23 INC., MONEYGRAM PAYMENT
SYSTEMS, INC., and FORCEPOINT LLC.

24 Defendants.

CASE NO.: 5:24-cv-404

CLASS ACTION

COMPLAINT FOR

- (1) Violation of the California Consumer Privacy Rights Act § 1798.150 *et seq.*; and
- (2) Invasion of Privacy, California Constitution Art. 1, § 1.

DEMAND FOR JURY TRIAL

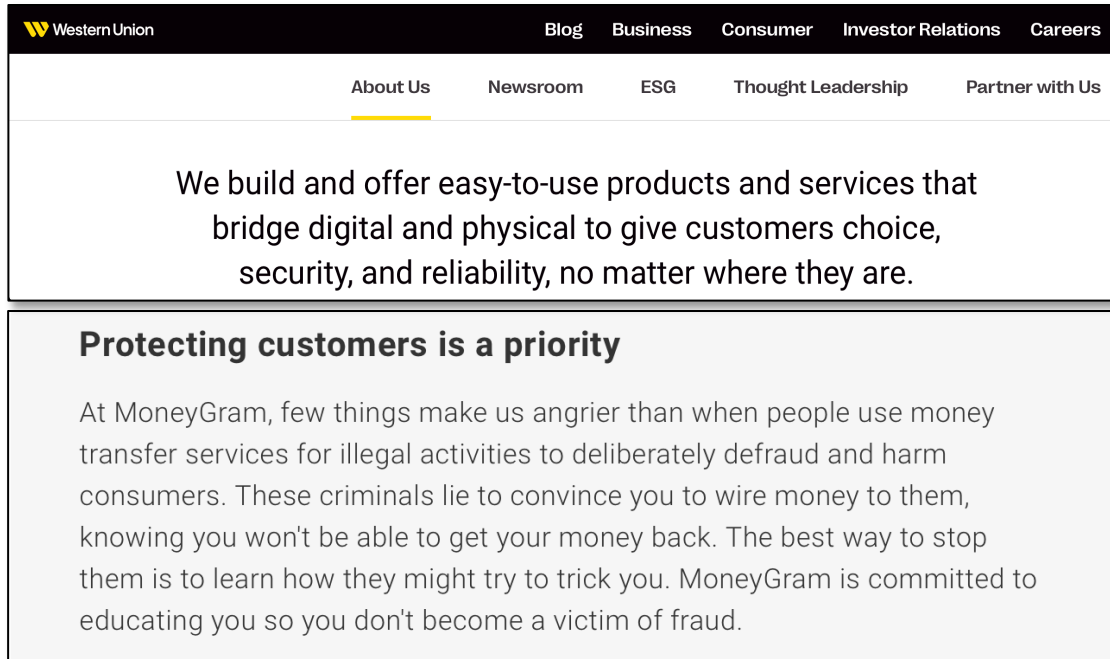
1 **CLASS ACTION COMPLAINT**

2 Plaintiffs Jose Guzman, Fortino Rutilo Jimenez, and Bertha Meza, on behalf
3 of themselves and all others similarly situated, by and through undersigned counsel,
4 file this Class Action Complaint against Western Union Financial Services, Inc.
5 (“Western Union”), MoneyGram International, Inc. and MoneyGram Payment
6 Systems, Inc. (“MoneyGram) (collectively, “Money Transfer Defendants”).
7 Plaintiffs Jose Guzman, Fortino Rutilo Jimenez, and Bertha Meza, on behalf of
8 themselves and all others similarly situated, also bring this Class Action Complaint
9 against Forcepoint LLC (“Forcepoint” or “Database Defendant”).

10 **NEED FOR ACTION**

11 1. The Money Transfer Defendants are in the business of providing money
12 transfer services to individual consumers, typically across international borders. As
13 part of these services, they are entrusted with the personal information of their
14 consumers. Much to their consumers’ detriment, that trust is wholly unwarranted.
15 As detailed below, the Money Transfer Defendants in coordination with the
16 Database Defendant voluntarily participated and continue to participate in a massive
17 and unlawful data dragnet collection and dissemination operation that compromises
18 the personal information of millions of unsuspecting consumers. Defendants’
19 outrageous conduct is contrary to their express legal obligations and their stated
20 commitment to protecting sensitive consumer information.

21 2. Indeed, each Money Transfer Defendants’ website emphasizes their
22 commitment to the privacy of the services they provide, stating things such as:
23
24
25
26
27
28



3. On January 15, 2023, the American Civil Liberties Union publicly released documents showing that Western Union and MoneyGram, in conjunction with state and federal actors, actively took part in a massive and unlawful dragnet data collection scheme to disclose their own consumers' personal information ("Protected Personal Information" as defined in Cal. Civ. Code § 1798.81.5(d)(1)(A)) to private actors, specifically Transaction Record Analysis Center, Inc. ("TRAC") and Forcepoint.

4. This unlawful data dragnet operation swept up Protected Personal Information related to Money Transfer Defendants' consumers who sent or received \$500 or more between Arizona, California, California, New Mexico, Texas, and the country of Mexico.

¹ <https://corporate.westernunion.com/> (last visited February 12, 2024).

² <https://www.moneygram.com/mgo/us/en/help/fraud-aware/fraud-prevention-information/> (last visited February 12, 2024).

1 5. The Protected Personal Information that Money Transfer Defendants
2 collected and disclosed was never sent to law enforcement. Instead, it was sent to
3 TRAC, an Arizona non-profit corporation whose tax filings indicate its stated
4 mission is: “[t]o educate law enforcement and industry to money laundering
5 technique and trends.” The Protected Personal Information was sent via Forcepoint,
6 TRAC’s database vendor.

7 6. As revealed in the ACLU press release, the Money Transfer Defendants
8 engaged in a years-long data dragnet collection and dissemination operation
9 premised on facially improper “administrative subpoenas” sent by the Arizona
10 Attorney General that cast an impermissible breadth and depth. In 2007, the Arizona
11 Court of Appeals found the Arizona Attorney General was improperly using the
12 administrative statute and that these types of “administrative subpoenas” were
13 invalid and illegal. These administrative subpoenas are just as invalid and illegal
14 today as they were in 2007.

15 7. Likewise, the Money Transfer Defendants’ data dragnet collection and
16 dissemination operation was also premised upon facially improper U.S. Immigration
17 and Customs Enforcement, Homeland Security Investigations (“HSI”) “customs
18 summonses,” which HSI withdrew after Senator Ron Wyden shined light on this
19 utterly invasive surveillance sweep on unsuspecting consumers.

20 8. After the Money Transfer Defendants gave Plaintiffs’ Protected
21 Personal Information to TRAC, TRAC used its database vendor Forcepoint to allow
22 law enforcement agencies around the country unfettered access to this Protected
23 Personal Information without a court order, warrant, or subpoena. Upon information
24 and belief, the Money Transfer Defendants’ and Database Defendant’s data dragnet
25 operation gave unfettered access to Plaintiffs’ Protected Personal Information to
26 over 700 law enforcement entities.

1 9. Plaintiffs were unaware that their Protected Personal Information was
2 being shared with third parties TRAC and Forcepoint, who were not disclosed as
3 third parties that may have access to Plaintiffs' Protected Personal Information.
4 Plaintiffs were likewise unaware that their Protected Personal Information was to be
5 indefinitely held in a data dragnet repository to be shared with further third parties,
6 including law enforcement agencies who were given access to the database without
7 warrant, subpoena, or court order. Plaintiffs did not consent to any such conduct.

8 10. Such an invasion of Plaintiffs' privacy is anathema to California law,
9 policy, and equity.

10 11. Accordingly, Plaintiffs Jose Guzman, Fortino Rutilo Jimenez, and
11 Bertha Gonzalez Meza on behalf of themselves and all others similarly situated,
12 bring this suit for statutory penalties, actual damages, and injunctive relief to avail
13 Plaintiffs and Class members of their constitutional and statutory privacy rights,
14 make Plaintiffs and Class members whole, and prevent this unconscionable conduct
15 from ever occurring again.

16 **I. PARTIES**

17 12. Plaintiff Jose Guzman is a natural person domiciled in California. He
18 resides in Chula Vista, California.

19 13. Plaintiff Fortino Rutilo Jimenez is a natural person domiciled in
20 California. He resides in Montebello, California.

21 14. Plaintiff Bertha Gonzalez Meza is a natural person domiciled in
22 California. She resides in Moreno Valley, California.

23 15. Defendant The Western Union Company also doing business as
24 Western Union Financial Services, Inc. ("Western Union") is a publicly-traded
25 Delaware corporation with its headquarters and principal place of business in
26 Englewood, Colorado. Western Union offers and provides remittances transfers to
27
28

1 consumers in 50 states, including California, and it regularly transacts and has
2 transacted business in this district.

3 16. Defendant MoneyGram International, Inc. (MGI) is a publicly-traded
4 Delaware corporation with its headquarters and principal place of business in Dallas,
5 Texas. MGI offers and provides remittance transfers to consumers in all 50 states,
6 including California, through its wholly-owned subsidiary MoneyGram Payment
7 Systems, Inc. (MPSI) (collectively, “MoneyGram”). MGI through its subsidiary
8 MPSI regularly transacts and has transacted business in this district.

9 17. Defendant Forcepoint LLC (“Forcepoint”) is a Delaware limited
10 liability company with its headquarters and principal place of business in Austin,
11 Texas. Forcepoint is registered to do business in the state of California
12 (201607910169) with a CA Registered Corporate Agent located at 7801 Folsom
13 Boulevard #202, Sacramento CA. Forcepoint, regularly transacts business in
14 California, including in this district.

15 **II. JURISDICTION AND VENUE**

16 18. This Court has subject matter jurisdiction over Plaintiffs’ claims
17 pursuant to 28 U.S.C. § 1332. The Court also has subject matter jurisdiction pursuant
18 to 28 U.S.C. § 1332(d)(2) because the amount in controversy exceeds \$5 million,
19 there are over 100 members in the proposed Class, and at least one member of the
20 proposed Class is a citizen of a state or country different from at least one Defendant.

21 19. This Court has personal jurisdiction over the Defendants because each
22 regularly transacts business in and throughout this district, and the wrongful acts
23 alleged in this Complaint were committed within this district.

24 20. Venue is proper in this District under 28 U.S.C. § 1391(b) because a
25 substantial part of the events or omissions giving rise to Plaintiffs’ claims occurred
26 in and emanated from this district.

1 **III. FACTUAL ALLEGATIONS**

2 **A. How Money Transfer Services and Transactions Work**

3 21. Western Union was founded in 1851 as a company operating primarily
4 in telegraph services, but eventually shifted its focus to cross-border money
5 transfers, largely marketing its services to immigrants. Similarly, MoneyGram was
6 formed to provide money transfer services to consumers globally.

7 22. Undeniably, this business model is based upon a booming market.
8 Money transfers, or remittances as they are often called, are estimated to grow by
9 1.4% to \$656 billion in 2023, up from \$647 billion in 2022.³ The United States is
10 one of the largest remitters and, notably, Mexico received the second highest level
11 of remittances in 2022.

12 23. As providers of money transfer services, the Money Transfer
13 Defendants' consumer base includes individuals spanning many countries and
14 commonly without bank accounts. Without a bank account, many individuals cannot
15 take advantage of electronic wire transfers or electronic checking to transfer money.
16 Or as is sometimes the case, money transfer services through providers such as the
17 Money Transfer Defendants are more cost-effective. In order to send money to a
18 distant place, consumers can use a money transfer service, such as those offered by
19 the Money Transfer Defendants to quickly send money abroad.

20 24. To earn a profit as a money transfer service, Money Transfer
21 Defendants charge fees related to each transaction, as well as by setting exchange
22 rates above market rate.

23
24
25 ³ The World Bank, *Remittances Remain Resilient but Likely to Slow*, June 13, 2023,
26 <https://www.worldbank.org/en/news/press-release/2023/06/13/remittances-remain-resilient-likely-to-slow> (last visited, February 12, 2024).
27

1 25. The money transfer process largely mirrors the following: (1) a sender
2 typically brings cash to a physical store where a representative of one of the Money
3 Transfer Defendants receives it and obtains information from the sender; (2) the
4 Money Transfer Defendants' representative also obtains information related to the
5 recipient of the money transfer and process the transaction; and (3) the recipient of
6 the transfer visits a physical location of the Money Transfer Defendants where the
7 money is delivered to them.

8 26. Consumers also transfer money using an online website or mobile
9 application that follows a similar process as outlined above, but done through a
10 similar online or mobile process.

11 **B. Western Union Cooperates With Unlawful Data Dragnet**
12 **Operation**

13 27. In 2006, the Arizona Attorney General served administrative subpoenas
14 under Arizona Revised Statute § 12-2315 and § 6-1242 seeking bulk transaction
15 data related to money transfers conducted through Western Union by its consumers.
16 The facially improper subpoenas sought data relating to every send and each receive
17 transaction of \$300 and greater received in the state of Sonora, Mexico, on a weekly
18 basis as each week becomes available, beginning with January 1, 2004 and ending
19 with December 31, 2006. The subpoena sought 49 separate data fields worth of
20 information for every \$300 or greater transaction over this two-year time period.

21 28. Western Union initially fought the enforcement of the subpoenas
22 against them, taking the enforceability question to the Arizona Court of Appeals.

23 29. A year later, in *State ex rel. Goddard v. Western Union Fin. Servs., Inc.*,
24 216 Ariz. 361 (App. 2007) the Arizona Court of Appeals held that the Attorney
25 General's subpoenas were unenforceable as a matter of law. The court found the
26 breadth of the subpoenas was impermissible and not reasonably articulated. In short,
27
28

1 the subpoenas violated the clear and well-defined principles of Fourth Amendment
2 particularity requirements, as well as similar requirements under Arizona law.

3 30. The Arizona Attorney General then brought suit against Western Union
4 under a state anti-money laundering law.

5 31. To settle the suit with the Arizona Attorney General, in 2010 Western
6 Union agreed to voluntarily produce, on an ongoing basis, its consumers' personal
7 identifying information (the "Western Union Settlement").

8 **1. Western Union Funds TRAC's Unlawful Data Dragnet**
9 **Operation**

10 32. In 2014, the Western Union Settlement was amended and expanded as
11 follows:

12 a. First, Western Union was required to deliver full transaction data
13 relating to all transactions sent to or from California, Arizona, New
14 Mexico, Texas, and the country of Mexico. Western Union was
15 required to continue sending this information over the next five years
16 until June 30, 2019.

17 b. Second, Western Union was required to pay hundreds of
18 thousands of dollars to establish and monetarily supplement the
19 Transaction Record Analysis Center, Inc. ("TRAC"), which would
20 house the data sent from Western Union. In fact, Western Union was
21 required to pay TRAC \$150,000 per month and also make a one-time
22 payment of \$250,000.00 to fund privacy, confidentiality, and
23 information security measures.

24 33. While early court records surrounding the Western Union Settlement
25 refer to TRAC as the "State Center," the incorporation, tax records, and funding by
26 Western Union state otherwise.

1 34. TRAC is not a governmental entity. Per its bylaws, TRAC was
2 incorporated in 2014 under the laws of Arizona as a non-profit corporation with the
3 purpose of promoting education, research, and training activities in the field of anti-
4 money laundering. Further, the bylaws hold that TRAC would receive funds and
5 research, train, and educate law enforcement agencies nationwide in the area of anti-
6 money laundering.

7 35. TRAC's tax filings confirm it is a 501(c)(3) non-profit, not a
8 government agency.

9 **2. TRAC Retains Forcepoint To Host Unlawful Data Dragnet**
10 **Operation**

11 36. According to a 2015 TRAC Data Policy, TRAC provides analytical and
12 data-related assistance to “need-to-know investigators, analysts, and prosecutors in
13 their efforts to disrupt criminal organizations and dismantle their operations by
14 providing resources, expertise, meaningful data analysis, training, and
15 organizational collaboration.” Moreover, TRAC provides law enforcement with
16 analytical and technical training regarding access to and the use of the TRAC system.

17 37. As an entity, TRAC maintains an electronic database of all the
18 Protected Personal Information it receives from Money Transfer Defendants. To
19 maintain the database, TRAC outsources its database software to Forcepoint and
20 other software database and/or cloud data service providers. Once users receive
21 training by TRAC, they have access to its database and requisite software interface.

22 38. Forcepoint is TRAC's principal software interface provider and
23 describes the TRAC system as “a centralized searchable database of the financial
24
25
26
27
28

1 transactions of global money services business [MSBs].”⁴ In providing this system,
2 Forcepoint acknowledges:

3 TRAC now serves as the intelligence component for [Arizona
4 Financial Crimes Task Force] and is staffed by analyst and law
5 enforcement professionals recognized as experts in money laundering
6 activity. The TRAC provides data, meaningful data analysis,
7 collaboration and training to investigators, analysts and prosecutors
8 nationwide in their efforts to disrupt criminal organizations and
9 dismantle their operations.⁵

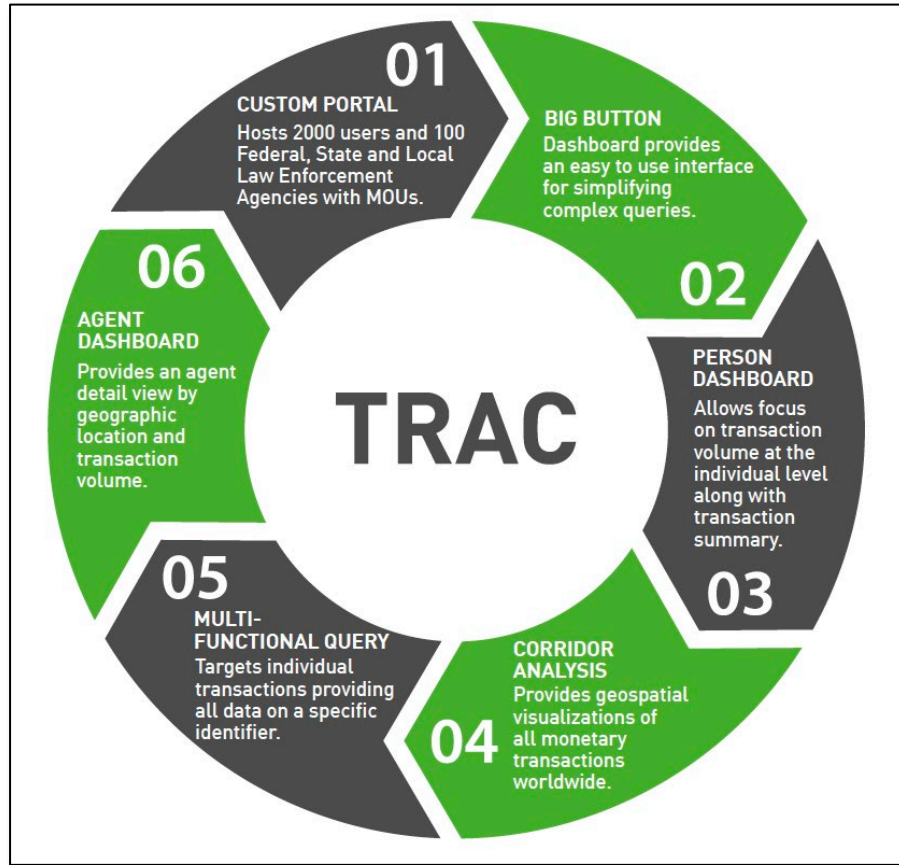
10 39. Tellingly, Forcepoint acknowledges the TRAC system is designed to
11 allow law enforcement agencies to circumvent ordinary constitutional protections
12 because the database contains “**more relevant data than what would be obtained in**
13 **a traditional subpoena process**” and is specifically designed to enable investigators
14 to avoid “**the usual subpoena process.**”⁶

23 ⁴ Forcepoint, *Case Study – Arizona Financial Crimes Task Force*,
24 [https://www.forcepoint.com/sites/default/files/case_study_downloads/casestudy_arizona_financi](https://www.forcepoint.com/sites/default/files/case_study_downloads/casestudy_arizona_financial_crimes_en_0.pdf)
25 [al_crimes_en_0.pdf](https://www.forcepoint.com/sites/default/files/case_study_downloads/casestudy_arizona_financial_crimes_en_0.pdf) (last visited on February 12, 2024).

26 ⁵ *Id.*

27 ⁶ *Id.*

1 40. Simply put, the TRAC system allows law enforcement to circumvent
 2 due process by collecting the Protected Personal Information of Plaintiffs and other
 3 innocent civilians to provide “visibility” into all monetary transactions worldwide:



18 41. In sum, TRAC, in association with Forcepoint, uses Protected Personal
 19 Information to create a database-to-software interface that operates much like a
 20 Google search: type in your relevant facts and return hits from consumers’ Protected
 21 Personal Information at the click of a button—no need to bother with the “lengthy
 22 delays in the usual subpoena process.”

23 **3. HSI Joins TRAC’s Unlawful Data Dragnet Operation**

24 42. Once the Western Union Settlement ended in 2019, HSI began issuing
 25 customs summons requesting Western Union transmit and disclose the Protected
 26 Personal Information data of its consumers directly to TRAC.
 27
 28

1 43. Based upon its litigation against the Arizona Attorney General, Western
2 Union was well aware that these types of data dragnet surveillance sweeps were
3 facially unlawful. The breadth of time range, number of data fields, and sheer
4 number of impacted consumers lacks articulation and specificity on its face. Indeed,
5 the Arizona Court of Appeals held as much.

6 44. Moreover, Western Union, as a sophisticated entity trading on the New
7 York Stock Exchange, knew or should have known the subpoenas from HSI were
8 patently violative of particularity requirements and unenforceable as a matter of law.

9 45. Nevertheless, Western Union voluntarily collected, compiled,
10 transmitted, and disclosed Plaintiffs' Protected Personal Information directly to
11 TRAC and/or Forcepoint in response to HSI's facially invalid customs summonses.

12 46. From 2019 to January 2022, HSI received 6,211,000 records from
13 Western Union and Maxi, another money transfer company.

14 47. In early 2022 after Senator Ron Wyden brought to light HSI's improper
15 use of customs summonses, HSI promptly withdrew them.

16 48. On information and belief, from 2019 to 2022 Western Union disclosed
17 Protected Personal Information of its consumers to the Database Defendant, with
18 categories similar to those requested from the Arizona Attorney General, including,
19 but not limited to, the following information for each send and receive transaction
20 over \$500 to or from California, Arizona, New Mexico, Texas, and the country of
21 Mexico:

- 22 a. (1) sender and receiver name, (2) sender and receiver address, (3)
23 sender and receiver city, (4) sender and receiver state, (5) sender and
24 receiver zip, (6) sender and receiver phone number, (7) sender and
25 receiver date of birth, (8) sender and receiver occupation, (9) sender
26 and receiver identification type, (10) sender and receiver identification
27 type description, (11) sender and receiver identification issuer, (12)
28

1 sender and receiver identification number, (13) sender and receiver
2 social security number;

3 b. For web based transfers: (1) Sender Internet Protocol Address
4 used during web account creation, (2) Sender Internet Protocol Address
5 used to send transaction, (3) send email address used to create web
6 based account, (4) sender email address used to send transaction, (5)
7 sender source account number, (6) sender name on web based account,
8 (7) sender included reasons for transaction.

9 49. On information and belief, Western Union continues to improperly
10 disclose Plaintiffs' Protected Personal Information to the Database Defendant.

11 50. Therefore, the Database Defendant continues to have access to
12 Plaintiffs' Protected Personal Information, causing Plaintiffs' Protected Personal
13 Information to be subject to disclosure to each and every law enforcement agency,
14 or any other person or entity, with access to the TRAC/Forcepoint system.

15 51. In voluntarily transmitting, transferring, and disclosing Plaintiffs'
16 Protected Personal Information to the Database Defendant, Western Union failed to
17 implement, uphold, or maintain reasonable security procedures and practices
18 appropriate to the nature of Plaintiffs' Protected Personal Information.

19 52. At no point did Western Union disclose to Plaintiffs that it would
20 collect, compile, transmit, or disclose Plaintiffs' Protected Personal Information
21 based upon unlawful requests or facially invalid subpoenas or summonses. Nor did
22 Plaintiffs consent to any such conduct.

23 53. At no point did Western Union disclose to Plaintiffs that it would
24 collect, compile, transmit, or disclose Plaintiffs' Protected Personal Information to
25 a third party non-profit named TRAC or Forcepoint. Nor did Plaintiffs consent to
26 any such conduct.

1 54. At no point did Western Union disclose to Plaintiffs that it had an
2 ongoing relationship with TRAC or Forcepoint, nor did Plaintiffs acknowledge or
3 consent to such relationship.


4 55. At no point did Western Union disclose to Plaintiffs that it would
5 collect, compile, transmit, or disclose Plaintiffs' Protected Personal Information to
6 undisclosed third parties or that the undisclosed third parties would permit an
7 additional subsequent disclosure to hundreds of law enforcement agencies without
8 any associated lawful request from such agencies. Nor did Plaintiffs consent to any
9 such conduct.

10 **C. MoneyGram Joins TRAC's Unlawful Data Dragnet Operation**

11 56. In 2019, while Western Union was turning over its own consumers
12 Protected Personal Information to the Database Defendant in conjunction with HSI
13 summonses, MoneyGram was regularly sent subpoenas from the Arizona Attorney
14 General under Arizona Revised Statute § 13-2315 seeking a trove of data related to
15 each money transfer.
16
17
18
19
20
21
22
23
24
25
26
27
28

1 57. An exemplar MoneyGram subpoena demonstrates the breadth of the
2 information sought:

3

4  **STATE OF ARIZONA**
OFFICE OF ATTORNEY GENERAL

5 2005 North Central Avenue
6 Phoenix, Arizona 85004
7 (602) 542-8431

8 **REQUEST TO PRODUCE RECORDS**

9

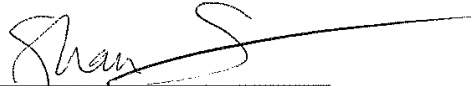
10 TO: MoneyGram Payment Systems
11 Attn: Melissa Grant ref. Law Enforcement Subpoena Compliance
12 1550 Utica Avenue South, Ste. 100
13 Minneapolis, MN 55416-5312

14 YOU ARE HEREBY COMMANDED, pursuant to A.R.S. § 13-2315, to produce
15 for examination and copying by the Attorney General of the State of Arizona the
16 following described records:

17 Data, including the data fields described on the attached Data Appendix, relating
18 to each send and each receive transaction of \$500 and greater, sent to or from the
19 states of Arizona, California, New Mexico, Texas and to or from the country of Mexico,
20 on a bi-weekly schedule as each such period becomes available, beginning with July 1,
21 2021 and ending with June 30, 2022. **(PLEASE INCLUDE THE ADDITIONAL DATA
22 FIELD FOR THE SUBPOENA IDENTIFICATION NUMBER. FOR THIS DATA FIELD
23 PLEASE INCLUDE REFERENCE NUMBER: AZAG2021RTP2)**

24 The data is to be delivered electronically to the Arizona Attorney General's Office
25 by delivery to its "SFTP" (Secure File Transfer Protocol) site in a delimited text files
26 format.

27 Please contact the Arizona Attorney General's Office through its investigator
28 Chad Brink at chad.brink@azag.gov for any questions regarding production of this
request and through its agent Mike Robinson at mike.robinson@forcepoint.com for the
secure VPN address, and to define a new CSV standard if necessary, for the data
delivery.


Shawn Steinberg
Assistant Attorney General
Arizona Attorney General's Office

1 58. The Arizona Attorney General continued to send these administrative
2 subpoenas to various money transfer entities from 2019 through at least 2022.

3 59. Notably, as shown above, these subpoenas from the Arizona Attorney
4 General required MoneyGram to remit the requested Protected Personal Information
5 directly to Forcepoint (TRAC's vendor), not the Arizona Attorney General.

6 60. From 2019 through 2022, MoneyGram received these subpoenas
7 requesting bulk transaction data for all transactions \$500 or greater that they serviced
8 between California, Arizona, New Mexico, Texas, and the country of Mexico for 6–
9 12 month periods, to be renewed with forthcoming subpoenas.

10 61. The subpoenas sought the following information:

11 a. (1) sender and receiver name, (2) sender and receiver address, (3)
12 sender and receiver city, (4) sender and receiver state, (5) sender and
13 receiver zip, (6) sender and receiver phone number, (7) sender and
14 receiver date of birth, (8) sender and receiver occupation, (9) sender
15 and receiver identification type, (10) sender and receiver identification
16 type description, (11) sender and receiver identification issuer, (12)
17 sender and receiver identification number, (13) sender and receiver
18 social security number;

19 b. For web based transfers: (1) Sender Internet Protocol Address
20 used during web account creation, (2) Sender Internet Protocol Address
21 used to send transaction, (3) send email address used to create web
22 based account, (4) sender email address used to send transaction, (5)
23 sender source account number, (6) sender name on web based account,
24 (7) sender included reasons for transaction.

1 62. To be clear, the Protected Personal Information was not sent by
2 MoneyGram to law enforcement. Instead, it was sent to Forcepoint, a vendor of
3 TRAC.

4 63. Neither TRAC nor Forcepoint are government entities.

5 64. As a sophisticated entity, MoneyGram knew or should have known that
6 the Arizona Attorney General’s subpoenas were patently and facially unenforceable
7 as demonstrated by the prior Arizona Court of Appeals opinion on virtually identical
8 facts.

9 65. Nevertheless, MoneyGram disclosed the requested Protected Personal
10 Information to the Database Defendant, from 2019 through at least 2022.

11 66. On information and belief, MoneyGram continues to disclose
12 Plaintiffs’ Protected Personal Information to the Database Defendant. Accordingly,
13 the Database Defendant continues to have access to Plaintiffs’ Protected Personal
14 Information.

15 67. Because the Database Defendant has access to Plaintiffs’ Protected
16 Personal Information, Plaintiffs’ Protected Personal Information is subject to
17 subsequent disclosure to each and every law enforcement agency, or other person,
18 with access to the TRAC/Forcepoint system.

19 68. In voluntarily collecting, compiling, transmitting, and disclosing
20 Plaintiffs’ Protected Personal Information, MoneyGram failed to implement,
21 uphold, or maintain reasonable security procedures and practices appropriate to the
22 nature of Plaintiffs’ Protected Personal Information.

23 69. At no point did MoneyGram disclose to Plaintiffs that they would
24 collect, compile, transmit, or disclose Plaintiffs’ Protected Personal Information
25 based upon unlawful requests or facially invalid subpoenas or summonses. Nor did
26 Plaintiffs consent to any such conduct.

1 70. At no point did MoneyGram disclose to Plaintiffs that they would
2 collect, compile, transmit, or disclose Plaintiffs' Protected Personal Information to
3 a third party non-profit named TRAC or Forcepoint. Nor did Plaintiffs consent to
4 any such conduct.

5 71. At no point did MoneyGram disclose to Plaintiffs that they had an
6 ongoing relationship with TRAC or Forcepoint, nor did Plaintiffs acknowledge or
7 consent to such relationship.

8 72. At no point did MoneyGram disclose to Plaintiffs that they would
9 collect, compile, transmit, or disclose Plaintiffs' Protected Personal Information to
10 undisclosed third parties or that the undisclosed third parties would permit an
11 additional subsequent disclosure to hundreds of law enforcement agencies without
12 any associated lawful request from such agencies. Nor did Plaintiffs consent to any
13 such conduct.

14 **IV. TOLLING OF STATUTE OF LIMITATIONS**

15 76. Plaintiffs and the other members of the Class had neither actual nor
16 constructive knowledge of the facts constituting their claim for relief. They did not
17 discover, nor could they have discovered through the exercise of reasonable
18 diligence, the existence of Money Transfer Defendants' and Database Defendant's
19 conduct until shortly before filing this Complaint.

20 77. The Money Transfer Defendants and Database Defendant failed to
21 reveal facts sufficient to put Plaintiffs and the other Class members on notice. Money
22 Transfer Defendants and Database Defendant did not and do not inform their
23 consumers that their consumers' Protected Personal Information would be sent to
24 TRAC or Forcepoint, nor that subsequent parties would have access to such
25 Protected Personal Information. Rather, Defendants give consumers false and
26 misleading impressions of security, safety, and privacy as mentioned in their
27 marketing.

1 78. At no point did Money Transfer Defendants or the Database Defendant
2 disclose to Plaintiffs that each would collect, compile, transmit, or disclose
3 Plaintiffs' Protected Personal Information as alleged herein. Nor did Plaintiffs
4 consent to any such conduct.

5 79. Moreover, an ordinary person acting reasonably diligent would not
6 have had the time, resources, or specialized training to uncover the misconduct that
7 Money Transfer Defendants or the Database Defendant engaged in here.

8 80. Indeed, Plaintiffs exercised reasonable diligence to protect their
9 Protected Personal Information from interception, exfiltration, or disclosure. To be
10 sure, that is precisely why Plaintiffs used Money Transfer Defendants' services—
11 fast, safe, and (allegedly) secure means of transmitting money to consumers abroad.

12 81. Due to the Money Transfer Defendants' and the Database Defendant's
13 fraudulent concealment of their wrongful conduct, the running of the statute of
14 limitations has been tolled and suspended with respect to the claims and rights of
15 action of Plaintiffs and the other Class members as a result of such conduct.

16 **V. FACTS SPECIFIC TO PLAINTIFFS**

17 82. Plaintiff Jose Guzman ("Guzman") regularly used Western Union to
18 send money from California to Mexico in 2020, including in excess of \$500.
19 Guzman was never informed his Protected Personal Information would be disclosed
20 upon an unlawful request nor that Guzman's Protected Personal Information would
21 be disclosed to an unidentified third party named TRAC or Forcepoint. Guzman was
22 never informed his Protected Personal Information would remain in a mass database
23 accessible by hundreds of government agencies or others. Guzman never consented
24 to any such disclosure of his Protected Personal Information. If Guzman had known
25 about this invasion of his privacy, he would not have paid Western Union to process
26 the transaction, and would instead have searched for alternative options for sending
27 his money. Guzman is disturbed that his Protected Personal Information, along with
28

1 information about friends abroad, was disclosed to the Database Defendant and
2 ultimately hundreds of law enforcement agencies without his knowledge. Guzman
3 seeks the full statutory and actual damages allowable under law.

4 83. Plaintiff Bertha Meza (“Meza”) regularly used Western Union to send
5 money from California to Mexico in 2022, including in excess of \$500. Meza was
6 never informed her Protected Personal Information would be disclosed upon an
7 unlawful request nor that Meza’s Protected Personal Information would be disclosed
8 to an unidentified third party named TRAC or Forcepoint. Meza was never informed
9 her Protected Personal Information would remain in a mass database accessible by
10 hundreds of government agencies or others. Meza never consented to any such
11 disclosure of her Protected Personal Information. If Meza had known about this
12 invasion of her privacy, she would not have paid Western Union to process the
13 transaction, and would instead have searched for alternative options for sending her
14 money. Meza is disturbed that her Protected Personal Information, was disclosed to
15 the Database Defendant and ultimately hundreds of law enforcement agencies
16 without her knowledge. Meza seeks the full statutory and actual damages allowable
17 under law.

18 84. Plaintiff Fortino Rutilo Jimenez (“Jimenez”) regularly used
19 MoneyGram to send money from California to Mexico in 2022, including in excess
20 of \$500. Jimenez was never informed his Protected Personal Information would be
21 disclosed upon an unlawful request nor that Jimenez’s Protected Personal
22 Information would be disclosed to an unidentified third party named TRAC or
23 Forcepoint. Jimenez was never informed his Protected Personal Information would
24 remain in a mass database accessible by hundreds of government agencies or others.
25 Jimenez never consented to any such disclosure of his Protected Personal
26 Information. If Jimenez had known about this invasion of his privacy, he would not
27 have paid MoneyGram to process the transaction, and would instead have searched
28

1 for alternative options for sending his money. Jimenez is disturbed that his Protected
2 Personal Information was disclosed to the Database Defendant and ultimately,
3 hundreds of law enforcement agencies without his knowledge. Jimenez seeks the
4 full statutory and actual damages allowable under law.

5 **VI. CLASS ACTION ALLEGATIONS**

6 **85. Class and Subclass Definitions:** Plaintiffs bring this action pursuant to
7 Fed. R. Civ. P. 23(b)(2) and (b)(3) on behalf of themselves and a Class and Subclass
8 of similarly situated individuals, defined as follows:

9 All California residents who used the services of any Money Transfer
10 Defendant or Money Transfer Defendants' subsidiaries or affiliates
11 and such residents' Protected Personal Information was sent to TRAC
and/or Forcepoint ("the Class").

12 All California residents whose Protected Personal Information was
13 sent to TRAC and/or Forcepoint and subsequently disclosed or
accessed. ("Database Defendant subclass").

14 The following people are also excluded from the Class and Subclass: (1) any Judge
15 or Magistrate presiding over this action and members of their families; (2) Money
16 Transfer Defendants and Database Defendant, as well as Money Transfer
17 Defendants' and Database Defendant's subsidiaries, parents, successors,
18 predecessors, and any entity in which the Money Transfer Defendants or Database
19 Defendant or their parents have a controlling interest, and their current or former
20 officers and directors; (3) persons who properly execute and file a timely request for
21 exclusion from the Class; (4) persons whose claims in this matter have been finally
22 adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel and
23 Defendants' counsel; and (6) the legal representatives, successors, and assigns of any
24 such excluded persons.

25 **86. Numerosity:** On information and belief, the proposed Class includes
26 hundreds of thousands, if not millions, of people. Members of the Class can be
27 identified through Money Transfer Defendants' and Database Defendant's records.

1 **87. Commonality and Predominance:** There are many questions of law
2 and fact common to Plaintiffs’ and each Class members’ claims, and those questions
3 predominate over any questions that may affect individual class members. Common
4 questions include but are not limited to the following:

- 5 a. Whether Plaintiffs and the Class members are “consumers”
6 under the California Consumer Privacy Rights Act, Cal. Civ.
7 Code § 1798.100 et seq.;
- 8 b. Whether Money Transfer Defendants and Database Defendant
9 are “businesses” under the California Consumer Privacy Rights
10 Act, Cal. Civ. Code § 1798.100 et seq.;
- 11 c. Whether the Money Transfer Defendants and Database
12 Defendant violated § 1798.150 of the California Consumer
13 Privacy Rights Act;
- 14 d. Whether the Money Transfer Defendants and Database
15 Defendant violated Plaintiffs’ and Class members’ privacy rights
16 in violation of the California Constitution;
- 17 e. Whether Plaintiffs and members of the Class are entitled to
18 injunctive relief, statutory damages, actual damages, and
19 reasonable costs and attorney’s fees from Money Transfer
20 Defendants and Database Defendant;
- 21 f. Whether Money Transfer Defendants and Database Defendant
22 should be enjoined from engaging in such conduct in the future;
23 and
- 24 g. The extent and form of any preliminary or equitable relief that
25 the Court determines appropriate.

26 **88. Typicality:** Plaintiffs’ claims are typical of the claims of other
27 members of the Class and Subclass in that Plaintiffs and the members of the Class
28

1 and Subclass were harmed, continue to be harmed, and Money Transfer Defendants’
2 and the Database Defendant’s conduct gave rise to the claims of Plaintiffs, the Class,
3 and the Subclass.

4 **89. Adequate Representation:** Consistent with Rule 23(a)(4), Plaintiffs
5 are adequate representatives of the Class because Plaintiffs are members of the Class
6 and committed to pursuing this matter against Money Transfer Defendants and the
7 Database Defendant to obtain relief for the Class. Plaintiffs have no conflicts of
8 interest with the Class. Plaintiffs’ counsel are competent and experienced in
9 litigating class actions, including extensive experience in litigating consumer claims.
10 Plaintiffs intend to vigorously prosecute this case and will fairly and adequately
11 protect the interests of the Class.

12 **90. Policies Generally Applicable to the Class:** This class action is
13 appropriate for certification because Defendants have acted on grounds generally
14 applicable to the Class as a whole, thereby requiring the Court’s imposition of
15 uniform relief to ensure compatible standards of conduct toward the members of the
16 Class and making final injunctive relief appropriate with respect to the Class as a
17 whole. The policies that Plaintiffs challenge apply to and affect members of the Class
18 uniformly, and Plaintiffs’ challenge of these policies hinges on Money Transfer
19 Defendants’ and the Database Defendant’s conduct with respect to the Class and
20 Subclass as a whole, not on facts or law applicable only to Plaintiffs. The factual and
21 legal bases of Money Transfer Defendants and Database Defendant liability to
22 Plaintiffs and to the other members of the Class and Subclass are the same.

23 **91. Predominance and Superiority:** Consistent with Rule 23(b)(3) the
24 questions of law or fact common to class members predominate over any questions
25 affecting only individual members, a class action is superior to any other available
26 means for the fair and efficient adjudication of this controversy, and no unusual
27 difficulties are likely to be encountered in the management of this class action. The
28

1 purpose of the class action mechanism is to permit litigation against wrongdoers
2 even when damages to individual plaintiffs and class members may not be sufficient
3 to justify individual litigation. Here, the damages suffered by Plaintiffs, the Class,
4 and Subclass members are relatively small compared to the burden and expense
5 required to individually litigate their claims against Money Transfer Defendants and
6 the Database Defendant, and thus, individual litigation to redress Money Transfer
7 Defendants' and the Database Defendant's wrongful conduct would be
8 impracticable. Individual litigation by each Class member and Subclass member
9 would also strain the court system. Moreover, individual litigation creates the
10 potential for inconsistent or contradictory judgments and increases the delay and
11 expense to all parties and the court system. By contrast, the class action device
12 presents far fewer management difficulties and provides the benefits of a single
13 adjudication, economies of scale, and comprehensive supervision by a single court.

14 **92. Injunctive and/or Declaratory Relief. Fed. R. Civ. P. 23(b)(2).**
15 Money Transfer Defendants and the Database Defendant through their uniform
16 conduct, acted or refused to act on grounds generally applicable to the Class as a
17 whole, making injunctive and/or declaratory relief appropriate.

18 93. Plaintiffs anticipate the issuance of notice, setting forth the subject and
19 nature of the instant action, to the proposed Class members. Upon information and
20 belief, Defendants' own business records, other available records, and/or electronic
21 media can be utilized for the contemplated notices. To the extent that any further
22 notices may be required, Plaintiffs anticipate the use of additional media and/or
23 mailings.

24 94. Plaintiffs reserve the right to revise each of the foregoing allegations
25 based on facts learned through additional investigation and in discovery.
26
27
28

1 **VII. CAUSES OF ACTION**

2 **COUNT 1**

3 **Violation of the California Consumer Privacy Rights Act § 1798.150 et seq.**
4 **(On behalf of Plaintiffs, the Class, and Subclass against All Defendants)**

5 95. Plaintiffs and Class members incorporate the foregoing paragraphs as
6 if set forth fully herein.

7 96. Plaintiffs bring this count on behalf of themselves and the Class.

8 97. The California Consumer Privacy Rights Act, § 1798.100, et seq.
9 (“CCPA”) is a comprehensive statutory scheme that is to be liberally construed to
10 empower and entitle Californians to know what personal information is collected
11 about them and whether their personal information is sold or disclosed and to whom.

12 98. Plaintiffs are “consumers” as defined by the CCPA.

13 99. The Money Transfer Defendants and the Database Defendant are
14 “businesses” as defined by the CCPA and therefore subject to liability thereunder.

15 100. The Money Transfer Defendants and the Database Defendant
16 compiled, held, and stored Plaintiffs’ Protected Personal Information as defined in
17 Cal. Civ. Code § 1798.81.5(d)(1)(A), including but not limited to Plaintiffs’ first and
18 last names, government identification, account numbers, and/or credit or debit card
19 numbers.

20 101. Plaintiffs’ Protected Personal Information was voluntarily collected,
21 stored, transmitted, and/or disclosed by Money Transfer Defendants and the
22 Database Defendant in a nonencrypted and nonredacted form, or in some other form
23 that permitted unauthorized individuals to access that information in violation of the
24 CCPA.

25 102. Through this voluntary disclosure, Money Transfer Defendants and the
26 Database Defendant breached their duty to implement, uphold, or maintain
27

1 reasonable security procedures and practices appropriate to the nature of Plaintiffs’
2 Protected Personal Information.

3 103. As a direct and proximate result of Money Transfer Defendants’ and
4 the Database Defendant’s failure to implement, uphold, or maintain reasonable
5 security procedures and practices appropriate to the nature of Plaintiffs’ Protected
6 Personal Information, Plaintiffs suffered unauthorized access, exfiltration, and
7 disclosure of Plaintiffs’ Protected Personal Information.

8 104. As a direct and proximate result of Money Transfer Defendants’ and
9 the Database Defendant’s unauthorized disclosure of Protected Personal
10 Information, Plaintiffs were injured and suffered violation of statutory privacy
11 interests.

12 105. In accordance with Cal. Civ. Code § 1798.150(b), prior to initiating this
13 suit, Plaintiffs’ counsel served Money Transfer Defendants and the Database
14 Defendant with proper notice of these CCPA violation via Federal Express.

15 106. Plaintiffs seek actual damages, statutory damages, costs, injunctive
16 relief, and attorney’s fees.

17 **COUNT 2**

18 **Invasion of Privacy Under California Constitution Art. 1, § 1**
19 **(On behalf of Plaintiffs, the Class, and Subclass against All Defendants)**

20 107. Plaintiffs incorporate the foregoing paragraphs as if set forth fully
21 herein.

22 108. Plaintiffs bring this count individually and on behalf of the members of
23 the Class and Subclass against the Money Transfer Defendants and Database
24 Defendant.

25 109. Plaintiffs, Class members, and Subclass members had a reasonable
26 expectation of privacy in the Protected Personal Information that Money Transfer
27 Defendants and Database Defendant disclosed without authorization.

1 110. Plaintiffs, Class members, and Subclass members have a strong interest
2 in: (1) precluding the dissemination or misuse of their sensitive Protected Personal
3 Information and related data; and (2) making personal decisions regarding the use
4 of their Protected Personal Information and related data, including the right to know
5 how such data may be used and to whom such data may be sent.

6 111. Money Transfer Defendants and the Database Defendant wrongfully
7 intruded upon Plaintiffs', Class members', and Subclass members' seclusion in
8 violation of California law. Plaintiffs' and Class members reasonably expected that
9 the Protected Personal Information and related data that they entrusted to Money
10 Transfer Defendants would be kept private and secure and would not be disclosed
11 to any unauthorized third party or for any improper purpose.

12 112. Money Transfer Defendants and the Database Defendant intentionally
13 invaded Plaintiffs', Class members', and Subclass members' privacy rights under
14 the California Constitution by:

- 15 a. obtaining, storing, remitting, and disclosing remitting Plaintiffs',
16 Class members', and Subclass members' Protected Personal
17 Information and related data to TRAC and Forcepoint, both
18 unauthorized, undisclosed third parties;
- 19 b. obtaining, storing, remitting, and disclosing Plaintiffs', Class
20 members', and Subclass members' Protected Personal Information
21 and related data to unauthorized, undisclosed third parties, to wit:
22 law enforcement;
- 23 c. enabling the disclosure of Protected Personal Information and
24 related data about Plaintiffs, Class members, and Subclass
25 members in a manner highly offensive to a reasonable person; and
26
27
28

1 d. enabling the disclosure of Plaintiffs', Class members', and Subclass
2 members' Protected Personal Information and related data without
3 their informed, voluntary, affirmative, and clear consent.

4 113. A reasonable person would find it highly offensive that Money Transfer
5 Defendants and the Database Defendant intentionally remitted Plaintiffs', Class
6 members', and Subclass members' Protected Personal Information and related data
7 to TRAC, Forcepoint, or any unauthorized third party without notice or consent to
8 do so.

9 114. Plaintiffs, Class members, and Subclass members did not consent to
10 any of Money Transfer Defendants' and the Database Defendant's alleged
11 misconduct, including any transfer or remittance of Plaintiffs', Class members', and
12 Subclass members' Protected Personal Information to TRAC or Forcepoint,
13 unauthorized and undisclosed third parties, or to any party thereafter following
14 Money Transfer Defendants' improper disclosures to TRAC and/or Forcepoint.

15 115. Money Transfer Defendants and the Database Defendant acted
16 knowingly or in reckless disregard of the fact that a reasonable person in Plaintiffs',
17 Class members', and Subclass members' position would consider all Defendants'
18 actions highly offensive.

19 116. Money Transfer Defendants and the Database Defendant were aware
20 that they were disclosing, transferring, or remitting Protected Personal Information
21 to unauthorized, undisclosed third parties and that doing so was not in response to a
22 lawful legal request.

23 117. Money Transfer Defendants' and the Database Defendant's unlawful
24 invasions of privacy damaged Plaintiffs and Class members. As a direct and
25 proximate result of these invasions, Plaintiffs, Class members, and Subclass
26 members suffered mental distress, and their reasonable expectations of privacy were
27 frustrated and defeated.

1 118. This invasion of privacy is serious in nature, scope, and impact.

2 119. This invasion of privacy constitutes an egregious breach of social
3 norms underlying the right to privacy.

4 120. Plaintiffs, Class members, and Subclass members therefore seek all
5 relief available for such invasion of privacy in violation of Article 1, § 1 of
6 California's Constitution.

7
8 **PRAYER FOR RELIEF**

9 Plaintiffs Jose Guzman, Fortino Rutilo Jimenez, and Bertha Meza,
10 individually and on behalf of all others similarly situated, respectfully request that
11 this Court enter an Order:

12 a) Certifying the Class under Rule 23 and naming the aforementioned
13 Plaintiffs as representatives of the Class and respective Subclasses and Plaintiffs'
14 attorneys as Class Counsel;

15 b) Declaring that Money Transfer Defendants' and Database Defendant's
16 conduct violates the laws and standards referenced above;

17 c) Finding in favor of Plaintiffs, the Class, and Subclass on all counts
18 asserted herein;

19 d) Enjoining Money Transfer Defendants and Database Defendant from
20 continuing to provide access to or copies of Plaintiffs', Class members', or Subclass
21 members Protected Personal Information, or otherwise not complying with the
22 CCPA.

23 e) Awarding Plaintiffs, Class members, and Subclass members statutory
24 damages for each violation of the CCPA;

25 f) Awarding Plaintiffs, Class members, and Subclass members actual
26 damages for each violation of the CCPA;

27 g) Awarding Plaintiffs, the Class, and the Subclass their reasonable
28

1 attorney's fees, expenses, and cost of suit;

2 h) Awarding pre- and post-judgment interest, to the extent allowable;

3 i) Requiring further injunctive and/or declaratory relief as necessary to
4 protect the interests of Plaintiffs and the Class; and

5 j) Awarding such other and further relief as equity and justice require.

6 **JURY DEMAND**

7 Plaintiffs request a trial by jury of all claims that can be so tried.

8 Dated: February 21, 2024

Respectfully submitted,

9
10 By: /s/ Taras Kick

11 Taras Kick (Cal. Bar No. 143379)

12 taras@kicklawfirm.com

13 Tyler Dosaj (Cal. Bar No. 306938)

tyler@kicklawfirm.com

14 **THE KICK LAW FIRM, APC**

815 Moraga Drive

15 Los Angeles, CA 90049

16 Tele: (310)395-2988

17 Fax: (310)395-2088

18 Daniel H. Charest (*pro hac vice* to be filed)

dcharest@burnscharest.com

19 Darren Nicholson (*pro hac vice* to be filed)

dnicholson@burnscharest.com

20 Chase Hilton (*pro hac vice* to be filed)

chilton@burnscharest.com

21 **BURNS CHAREST, LLP**

22 900 Jackson Street, Suite 500

23 Dallas, TX 75202

24 Tele: (469)904-4550

25 Fax: (469)444-5002

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Western Union, MoneyGram Lawsuit Says Cos. Shared Money Transfer Data with Law Enforcement Group](#)
