UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairman**
Jon Leibowitz
Julie Brill
Maureen K. Ohlhausen
Joshua D. Wright

In the Matter of	)	
DECEMBER 12, 2012 CIVIL INVESTIGATIVE DEMAND ISSUED TO THE WESTERN UNION COMPANY	)	**File No. 012 3145**
AND	)	**March 4, 2013**
NOVEMBER 5, 2012 CIVIL INVESTIGATIVE DEMAND ISSUED TO LONNIE KEENE, MONITOR, STATE OF ARIZONA V. WESTERN UNION FINANCIAL SERVICES, INC.	)	**Redacted Public Version**

ORDER DENYING PETITION TO QUASH
CIVIL INVESTIGATIVE DEMANDS

By OHLHAUSEN, Commissioner:

Western Union Company ("Western Union") has filed a petition to quash civil investigative demands ("CIDs") issued by the Federal Trade Commission ("FTC" or "Commission") to Western Union and to Mr. Lonnie Keene, an independent monitor appointed pursuant to Western Union's settlement of money laundering charges by the State of Arizona. *See Arizona v. Western Union Financial Services, Inc.*, No. CV 2010-5807 (Ariz. Super. Ct. Maricopa Cnty. Feb. 24, 2010). For the reasons stated below, the petition is denied.

I. BACKGROUND

Over the past several years, money transfers have become the payment method of choice for those seeking to defraud consumers in the U.S. and abroad. There are several reasons for this development. First and foremost, a money transfer through companies

like Western Union or MoneyGram is essentially the same as sending cash. Thus, consumers have no chargeback rights, as they would have if they had paid by credit card. A money transfer also enables the perpetrators of a scheme to get consumers' funds quickly. Indeed, a money transfer can be picked up by the recipient within a matter of minutes at multiple locations virtually anywhere in the world, rather than a single designated location. In many instances, the recipient is not even required to provide identification. All of these factors make it extremely difficult for the FTC and other enforcement agencies to identify and take action against perpetrators of frauds that employ money transfers.

The FTC continues to receive a high volume of complaints about fraudulent and deceptive practices that rely on money transfers as the method of payment. In 2012 alone, the FTC's database of consumer complaints ("Consumer Sentinel") received more than 102,000 complaints from consumers who lost money through a fraud-induced money transfer, with reported losses exceeding $450 million. In the same year, money transfers were by far the most common payment method for consumers complaining of fraudulent or deceptive practices, accounting for 47% of all Consumer Sentinel complaints that reported a method of payment.[1] In many of these schemes perpetrators outside the U.S. target U.S. consumers.

Money transfer companies can play an important role in addressing the use of money transmission services to facilitate fraud. They can often identify suspicious outlets, locations, or agents, and can detect patterns of transactions consistent with ongoing fraudulent and deceptive practices. Through diligent and effective antifraud policies and procedures, these companies can address and deter those activities. For example, as required by the consent order in *FTC v. MoneyGram Int'l, Inc.*, No. 09-cv-6576 (N.D. Ill. Oct. 19, 2009), MoneyGram must establish, implement, and maintain a comprehensive antifraud program that "is reasonably designed to protect Consumers by detecting and preventing Fraud-Induced Money Transfers *worldwide* and to avoid installing and doing business with MoneyGram agents *worldwide* who appear to be involved in or complicit in processing Fraud-Induced Money Transfers."[2]

Following the consent order with MoneyGram, FTC staff asked Western Union to provide, on a voluntary basis, information about steps the company was taking to reduce

[1] *See* FTC, Consumer Sentinel Network Data Book for January – December 2012, at 8 (Feb. 2013), *available at* http://ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012.pdf.

[2] Stipulated Order for Permanent Injunction and Final Judgment at 7-8, *FTC v. MoneyGram Int'l, Inc.*, No. 09-cv-6576 (N.D. Ill. Oct. 19, 2009) (emphasis added).

fraud-induced money transfers. In June 2012, FTC staff requested that Western Union voluntarily provide the FTC with reports produced by a monitor appointed pursuant to an agreement with the State of Arizona that settled charges that Western Union's money transfer business was being used to facilitate human smuggling or narcotics trafficking.

After Western Union refused to provide the reports voluntarily,[3] the Arizona Attorney General sought an order clarifying that the terms of the settlement were broad enough to allow Arizona to share the Monitor's reports with the FTC.[4] The reports had been filed under seal (and therefore kept off the public record) pursuant to a provision in the Settlement Agreement allowing – but not requiring – either Western Union or the Arizona Attorney General to request that the reports be filed under seal.[5]

The state court denied the Arizona Attorney General's request, without prejudice, on September 25, 2012. The ruling was premised on the court's view that "for the Court to order disclosure to [the FTC and Department of Homeland Security] pursuant to the agreement, I would want them in the courtroom to know what the scope of the agreement is, that it is going to be a two-way street. It would benefit the monitor in doing the monitor's job."[6] The court made clear that it was making no comment on "the extent that the FTC or Homeland Security has a right to secure information that the monitor has or the Attorney General's Office has."[7]

The Commission then issued CIDs to obtain the reports and related materials, first to the Monitor and then to Western Union directly. Specifically, on November 5, 2012,

---

[3] Western Union did provide other information about its antifraud program and contributed complaints from U.S.-based consumers to the Commission's online complaints database. Starting in August 2012, FTC staff also requested foreign complaints, but Western Union declined based on privacy concerns.

[4] Pet. Ex. E. The Arizona Attorney General pointed out that such a release is consistent with the Monitor Engagement Letter ("MEL") (*see* Pet. Ex. E, at 5-6; *see also* Pet. Ex. B ¶ 9) and is specifically authorized by Paragraph 17.1.4 of the Settlement Agreement (providing that the state has leave to disclose any materials or information provided by Western Union where such disclosure "is required by law, otherwise authorized by this Agreement, or is in the proper discharge of or otherwise furthers the State's official duties or responsibilities.").

[5] Pet. Ex. D, at 4.

[6] Pet. Ex. F, at 21-22.

[7] Pet. Ex. F, at 21.

the Commission issued a CID to the Monitor, seeking

> All documents referring or relating to the Periodic Reviews of the Monitor appointed by the court in *State of Arizona ex rel. Horne v. Western Union Financial Services, Inc.*, No. CV 2010-005807, including, but not limited to, all drafts of any reports, reviews, or correspondence with Western Union.

The Commission directed a separate CID to Western Union on December 12, 2012. In addition to the Monitor's reports, the CID requires Western Union to produce (1) internal documents that refer or relate to communications with the Monitor – *i.e.*, documents showing Western Union's internal reaction to the findings and recommendations in the Monitor's reports; and (2) complaints from consumers worldwide referring or relating to fraud-induced transactions. As defined, such complaints include complaints made by foreign consumers about transactions that were picked up either in the U.S. or in a foreign jurisdiction.

After receiving the CID, the Monitor sought to confirm his authority to provide the requested materials to the FTC by filing a motion in the settled Arizona action. On January 28, 2013, the state court denied that request "in the absence of a formal enforcement action order issued by the appropriate federal jurisdiction."[8] The court reasoned that Western Union had an expectation of confidentiality when it "voluntarily gave the Monitor access to its otherwise private practices and proprietary data." Accordingly, the court concluded, it was reasonable "that Western Union did not expect that [its] proprietary information and practices would be otherwise provided to a third party who has no enforceable limitation on its use or disclosure."[9] The state court specifically noted that (1) "it has no jurisdiction, and makes no attempt to determine the enforceability of the FTC's CID," and (2) it was "in no way address[ing] the issue of whether the FTC has authority to take" the Monitor's reports and what the FTC "may do with them."[10]

On January 31, 2013, Western Union filed the instant petition to quash.[11]

---

[8] Pet. Ex. G, at 4.

[9] Pet. Ex. G, at 2-3.

[10] Pet. Ex. G, at 3-4.

[11] It is by no means certain that Western Union has standing to seek to quash the CID issued to the Monitor. Generally, the target of a government investigation lacks standing to dispute the validity of administrative subpoenas directed to a third party. *See, e.g., Greene v. Phila. Hous. Auth.*, 789 F. Supp. 2d 582, 586 (E.D. Pa. 2011); *see also*

II. ANALYSIS

A. The Applicable Legal Standards.

Compulsory process such as a CID is proper if the inquiry is within the authority of the agency, the demand is not too indefinite and the information sought is reasonably relevant to the inquiry, as defined by the Commission's investigatory resolution.[12] Agencies have wide latitude to determine what information is relevant to their law enforcement investigations and are not required to have "a justifiable belief that wrongdoing has actually occurred."[13]

Western Union argues that the CIDs should be quashed because they do not satisfy these standards. First, Western Union claims that the CIDs were not issued pursuant to a valid resolution. Second, Western Union claims that the requested materials are not relevant to the purpose of the investigation. Third, it claims that the FTC lacks authority to compel the production of materials prepared pursuant to, or as a consequence of, a state court settlement. Fourth, Western Union contends that the Commission exceeded its authority in seeking complaints and information related to money transfers between foreign countries. As explained below, we are not persuaded that these contentions have merit.

FTC v. Trudeau, 2012 U.S. Dist. LEXIS 160545, at *8 (N.D. Ohio Nov. 8, 2012). Western Union contends that its privacy interests are sufficient to confer standing. Pet. 7 n.3. We note, however, that Western Union's claimed privacy interests are inconsistent with the terms of the MEL. *See* Pet. Ex. B ¶ 5 ("The Monitor shall be independent of Western Union and the State, and no attorney-client relationship shall be formed between them."). Thus, the decision of the Sixth Circuit in *American Motors Corp. v. FTC*, 601 F.2d 1329, 1338-39 (6th Cir. 1979), cited by petitioner, is questionable authority for Western Union's assertion that it has retained "privacy rights." Pet. 7 n.3. In any event, even if Western Union has an interest that is sufficient to confer standing, its petition to quash the Monitor's CID is without merit for the reasons discussed herein.

[12] *United States v. Morton Salt Co.*, 338 U.S. 632, 652 (1950); *FTC v. Invention Submission Corp.*, 965 F.2d 1086, 1089 (D.C. Cir. 1992); *FTC v. Texaco, Inc.*, 555 F.2d 862, 874 (D.C. Cir. 1977).

[13] *See, e.g., Morton Salt*, 338 U.S. at 642-43 ("[Administrative agencies have] a power of inquisition, if one chooses to call it that, which is not derived from the judicial function. It is more analogous to the Grand Jury, which does not depend on a case or controversy for power to get evidence but can investigate merely on suspicion that the law is being violated, or even just because it wants an assurance that it is not.").

B. The CIDs Are Supported by a Specific and Valid Resolution.

Western Union's contention that the resolution would permit the FTC to investigate any party "engaged in sales with respect to any form of practice or conduct" is not borne out by the text of the resolution. In issuing the CIDs, the Commission relied on omnibus resolution No. 0123145, *Resolution Directing Use of Compulsory Process in a Nonpublic Investigation of Telemarketers, Sellers, Suppliers, or Others* (Apr. 11, 2011). The resolution authorizes the use of compulsory process to determine whether telemarketers, sellers, or others assisting them have or are violating Section 5 of the FTC Act, 15 U.S.C. § 45, or the Telemarketing Sales Rule, 16 C.F.R. Part 310.[14] The resolution also provides specific notice that it pertains to investigations relating to telemarketing activities, and includes investigations of telemarketers or sellers as well as entities such as Western Union who may be providing substantial assistance or support to telemarketers or sellers.

This statement of the purpose and scope of the investigation is more than sufficient under applicable standards, and courts have enforced compulsory process issued under similar resolutions.[15] Indeed, this resolution has been in effect for many years and has

---

[14] The resolution describes the nature and scope of the investigation as follows:

> To determine whether unnamed telemarketers, sellers, or others assisting them have engaged in or are engaging in: (1) unfair or deceptive acts or practices in or affecting commerce in violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 (as amended); and/or (2) deceptive or abusive telemarketing acts or practices in violation of the Commission's Telemarketing Sales Rule, 16 C.F.R. pt 310 (as amended), including but not limited to the provision of substantial assistance or support – such as mailing lists, scripts, merchant accounts, and other information, products, or services – to telemarketers engaged in unlawful practices. The investigation is also to determine whether Commission action to obtain redress for injury to consumers or others would be in the public interest.

Resolution Directing Use of Compulsory Process in a Nonpublic Investigation of Telemarketers, Sellers, Suppliers, or Others, File No. 0123145 (Apr. 11, 2011).

[15] *See* Opinion and Order at 11-12, *FTC v. LabMD, Inc.*, No. 1:12-cv-3005-WSD (N.D. Ga. Nov. 26, 2012); *FTC v. Nat'l Claims Serv., Inc.*, 1999 WL 819640, at *2 (E.D. Cal. Feb. 9, 1999) (approving use of omnibus resolution citing provisions of the FTC Act and the Commission's Franchise Rule); *FTC v. O'Connell Assocs., Inc.*, 828 F. Supp. 165, 171 (E.D.N.Y. 1993) (enforcing CIDs issued pursuant to omnibus resolution citing provisions of the FTC Act and the Fair Credit Reporting Act). The Commission has

supported multiple other investigations, including CIDs issued to Western Union's competitor, MoneyGram, in 2007 and 2008.

Western Union's reliance on the decision of the D.C. Circuit in *FTC v. Carter*, 636 F.2d 781, 788 (D.C. Cir. 1980), is misplaced. Although *Carter* held that a bare reference to Section 5 of the FTC Act, without more, "would not serve very specific notice of purpose," the Court approved the resolution at issue, noting that it also referred to specific statutory provisions of the Cigarette Labeling and Advertising Act, and further related it to the subject matter of the investigation.[16] With this additional information, the Court felt "comfortably apprised of the purposes of the investigation and the subpoenas issued in its pursuit."[17] Similarly, the resolution here provides substantially more information than the bare text of Section 5, and thus adequately notifies Western Union of the nature and scope of the investigation.

Western Union's argument also fails in light of the history of communications between the company and the FTC. The purpose of an authorizing resolution is to notify a CID recipient of the nature and scope of the investigation.[18] Given the lengthy dialogue between staff and Western Union, there is no doubt that the company is aware of the nature of staff's investigation. The Commission has previously found that such interactions may be considered along with the resolution in evaluating the notice provided to Petitioners: "[T]he notice provided in the compulsory process resolutions, CIDs, and other communications with Petitioner more than meets the Commission's obligation of providing notice of the conduct and the potential statutory violations under investigation."[19]

---

repeatedly rejected similar arguments about such omnibus resolutions. *See, e.g.*, *LabMD, Inc*., No. 123099, at 9 (Apr. 20, 2012); *Firefighters Charitable Found*., No. 102-3023, at 4 (Sept. 23, 2010); *D.R. Horton, Inc*., Nos. 102-3050, 102-3051, at 4 (July 12, 2010); *CVS Caremark Corp.*, No. 072-3119, at 4 (Dec. 3, 2008).

[16] *Carter*, 636 F.2d at 788.

[17] *Id.* Western Union also contends that the resolution fails to conform to the FTC's Operating Manual. Pet. 9. But for the reasons stated above, the resolution at issue is sufficiently specific to comply with the Operating Manual. FTC Operating Manual, Ch. 3.3.6.7.4.1. In any event, the manual itself confers no rights on Western Union. *Id.*, Ch. 1.1.1; *see also FTC v. Nat'l Bus. Consultants, Inc.*, 1990 U.S. Dist. LEXIS 3105, 1990-1 Trade Cas. (CCH) ¶ 68,984, at *29 (E.D. La. Mar. 19, 1990).

[18] *O'Connell Assocs., Inc.*, 828 F. Supp. at 170-71.

[19] *Assoc. First Capital Corp.*, 127 F.T.C. 910, 915 (1999).

C. The Documents Sought Are Relevant to the Commission's Investigation.

Western Union claims that the CID specification calling for the Monitor's reports and related documents is irrelevant to the FTC's investigation into consumer fraud and telemarketing. Specifically, Western Union claims that the Monitor's reports relate to human and drug trafficking in the Southwest border area and that these issues are far outside the stated purposes of the FTC's investigation.[20]

In the context of an administrative CID, "relevance" is defined broadly and with deference to an administrative agency's determination.[21] An administrative agency is to be accorded "extreme breadth" in conducting an investigation.[22] As the D.C. Circuit has stated, the standard for judging relevance in an administrative investigation is "more relaxed" than in an adjudicatory proceeding.[23] As a result, the agency is entitled to the documents unless the CID recipient can show that the agency's determination is "obviously wrong" or the documents are "plainly irrelevant" to the investigation's purpose.[24] We find that Western Union has not met this burden.

Although Western Union tries to couch the settlement and the Monitor's tasks as relating to human or drug trafficking, a review of the Monitor Engagement Letter shows that it is more general and relates to oversight by the Monitor of Western Union's anti-money laundering ("AML") program as required by the Bank Secrecy Act ("BSA") and related guidance.[25] The statutory and regulatory provisions relating to Western Union's

---

[20] Pet. 13-14.

[21] *FTC v. Church & Dwight Co., Inc.*, 665 F.3d 1312, 1315-16 (D.C. Cir. 2011); *FTC v. Ken Roberts Co.*, 276 F.3d 583, 586 (D.C. Cir. 2001).

[22] *Linde Thomsen Langworthy Kohn & Van Dyke, P.C. v. RTC*, 5 F.3d 1508, 1517 (D.C. Cir. 1993).

[23] *Invention Submission Corp.*, 965 F.2d at 1090.

[24] *Id.* at 1089; *Carter*, 636 F.2d at 788. We note that Western Union has not contested the relevance of the worldwide complaints that are the subject of Specification 1. Its arguments on relevance are limited to the Monitor's reports and related documents sought under Specification 2.

[25] "To ensure that its Program adheres to the principles enunciated in the Financial Action Task Force Risk-Based Approach to Combating Money Laundering and Terrorist Financing ('FATF RBA Guidance'), to its legal obligations, to the Agreement, and to this

money services business ("MSB") authorities do not segregate AML and antifraud programs. Western Union is required by the BSA and its implementing regulations to implement an AML program,[26] which includes filing Suspicious Activity Reports ("SARs") for "possible violation[s] of law or regulation."[27] Those reports are not limited to money laundering. Instead, the BSA is clear that the SARs required from Western Union's AML program must report *any* type of suspicious transaction, including consumer fraud.[28] Indeed, in guidance published to examiners of money services businesses for compliance with the BSA, the Department of the Treasury made it plain that an AML program must detect and report on transactions that involve more than just money laundering, and that the business itself should not try to distinguish one type of illegal conduct from another for purposes of its reporting requirement:

> MSBs are required to report suspicious activities above prescribed dollar thresholds that may involve money laundering, BSA violations, terrorist financing, *and certain other crimes*. However, MSBs cannot be expected and are not required to investigate or confirm the underlying crime (e.g., terrorist financing, money laundering, tax evasion, identity theft, *or fraud*).[29]

Thus, from a regulatory perspective, there is substantial overlap between an AML program and a program to detect consumer fraud and other illegal activities. Indeed, until the summer of 2012, Western Union's AML and antifraud personnel were housed within the same corporate group, meaning that a common set of personnel were involved in

---

Monitor Engagement Letter, Western Union has agreed to be overseen by an independent Monitor . . . ." Pet. Ex. B ¶ 2.

[26] 31 U.S.C. §§ 5312(a)(2)(R), 5318(h); 31 C.F.R. § 1022.210(d).

[27] 31 U.S.C. § 5318(g); 31 C.F.R. § 1022.320(a).

[28] 31 U.S.C. § 5318(g) ("The Secretary may require any financial institution, and any director, officer, employee, or agent of any financial institution, to report any suspicious transaction relevant to a possible violation of law or regulation."); 31 C.F.R. § 1022.320(a) ("Every money services business . . . shall file with the Treasury Department, to the extent and in the manner required by this section, a report of any suspicious transaction relevant to a possible violation of law or regulation.").

[29] Fin. Crimes Enforcement Network & Internal Revenue Serv., Bank Secrecy Act/Anti-Money Laundering Examination Manual for Money Services Businesses 86 (2008) (emphasis added) (footnote omitted), *available at* http://www.fincen.gov/news_room/rp/files/MSB_Exam_Manual.pdf.

responding to complaints of consumer fraud as well as suspected money laundering activity.

The overlap is further demonstrated by a comparison of the Monitor's obligations for overseeing the AML program, as outlined in the MEL, and Western Union's antifraud program, as described in the overview document that Western Union provided to FTC staff in September 2012.[30] For example, the Monitor is required to evaluate whether Western Union's AML program, among other things:

- Provides for adequate oversight and controls of Agents, consumers, transactions, products, services, and geographic areas that are more vulnerable to abuse by money launderers and other criminals;
- Provides for regular review of the risk assessment and risk management processes;
- Contains channels for informing senior management of compliance initiatives, compliance deficiencies, corrective actions, and filing of suspicious activity reports;
- Provides for appropriate initial and refresher training for Agents to be given at appropriate intervals.[31]

None of these tasks is unique to anti-money laundering activities. Indeed, the same tasks are specifically mentioned in Western Union's Anti-Fraud Program overview.[32]

Similarly, the Monitor is charged with developing an "Implementation Plan" that includes the Monitor's own recommendations for Western Union and that presumptively includes certain "existing measures" already employed by Western Union as part of its

---

[30] Letter from John R. Dye, EVP, Gen. Counsel & Sec'y, Western Union, to David Vladeck, Dir., Bureau of Consumer Prot., FTC (Sept. 14, 2012) [hereinafter Anti-Fraud Program].

[31] Pet. Ex. B, at 6-7.

[32] *See, e.g.*, Anti-Fraud Program 7 [redacted]; *id.* at 4 [redacted] *id.* at 5-6 [redacted] *id.* at 23-24 [redacted].

AML program.[33] Many of these existing AML measures are also part of Western Union's antifraud program, as described in the company's own materials:

- One of the "existing measures" for the AML program is "developing the ability to aggregate consumer transactions to identify unusual activity on a real-time basis (through its Real Time Risk Assessment initiative)."[34] [redacted].[35]

- Another "existing measure" is "developing, to the extent reasonably feasible, Real Time Risk Assessment that will provide the ability to block noncompliant transactions before they are processed, so that when a transaction violates established business rules, a 'pop-up screen' will immediately notify the Agent that the transaction cannot be completed."[36] [redacted][37]

- A third "existing measure" is "implementing Transaction Risk Index ('TRI') model variables and formulas . . . to more strategically mitigate the risks associated with certain geographies (e.g., Arizona) and 'red flags' such as structuring, sharing of consumer identifying information, high volume, high frequency, and SARs filed

---

[33] Pet. Ex. B ¶¶ 18-23. Specifically, paragraph 23 of the MEL, entitled "Presumed Program Measures," provides that Western Union's existing AML measures will become part of the Monitor's recommendations "unless the Monitor, with input from Western Union and the State, determines that it is not technically feasible or would not improve the Program." Pet. Ex. B ¶ 23.

[34] Pet. Ex. B ¶ 23.1.2.

[35] Anti-Fraud Program 14-16 [redacted].

[36] Pet. Ex. B ¶ 23.1.8.

[37] Anti-Fraud Program 4.

by Western Union on transactions facilitated by/through the Agent."[38] [redacted][39]

We conclude, therefore, that the steps Western Union must take to eliminate various forms of any suspected illegal transactions from its system are essentially the same. Both the AML and antifraud programs are intended to prevent illegal transactions occurring through the company's money transfer system, and both programs employ similar tools to do so: analysis of transaction data to identify patterns, computer-based rules that prevent illegal transactions from entering the system, training to help agents identify illegal transactions, and disciplinary action against agents that are complicit in the illegal activity or continue to generate high levels of complaints.[40] To the extent the Monitor's reports include an assessment of, and recommendations for, each of these facets of Western Union's AML program, they are highly relevant to the current inquiry into the adequacy of the company's antifraud program.[41]

It is also important to note that the CID directed to Western Union is not limited to the Monitor's reports. Rather, the CID requests "[a]ll documents referring or relating to

---

[38] Pet. Ex. B ¶ 23.1.5.

[39] Anti-Fraud Program 3.

[40] To provide another example of the overlap between Western Union's AML and antifraud programs: one of the key issues identified in the Arizona action was Western Union's awareness of, and failure to terminate, complicit U.S. and foreign agents who "were knowingly engaged in a pattern of money laundering violations." *See* Settlement Agreement Ex. A ("Statement of Admitted Facts"), *Arizona v. W. Union Fin. Servs., Inc.*, No. CV 2010-5807 (Ariz. Super. Ct. Maricopa Cnty. Feb. 24, 2010), *available at* https://www.azag.gov/sites/default/files/sites/all/docs/swbamla/State%20of%20Arizona%20v.%20Western%20Union%20Settlement%20Agreement%20compact.pdf. [redacted] Anti-Fraud Program 4.

[41] The Monitor's reports are also uniquely valuable because they provide the perspective of an independent third party who owes no duties to Western Union. Indeed, to ensure the Monitor's independence, the MEL specifies that neither Western Union nor the State of Arizona shall provide any personal benefit to the Monitor during the term of the Monitor's engagement or for five years afterward. Pet. Ex. B ¶ 4.

communications with the Monitor."[42] The CID thus encompasses Western Union's internal communications and reactions to the findings and recommendations of the Monitor, which are relevant to determining the strength of the company's culture of compliance and whether there is a widespread commitment to eliminating illegal transactions from Western Union's system. These documents, which have not been shared with the Monitor or with the Arizona Attorney General, are not covered by any confidentiality provisions in the settlement documents and thus must be produced in response to the CID directed at Western Union.

In short, the Monitor's reports and related materials are relevant to assessing Western Union's commitment to eliminating illegal transactions from its system, and thus are "reasonably relevant" to the purposes of the Commission's investigation. Western Union has not satisfied its burden to demonstrate that the information requested by the CID is "plainly irrelevant" or "obviously wrong."[43]

D. The CIDs Are Valid Exercises of the Commission's Authority.

1. The FTC Has Authority to Obtain the Monitor's Reports and Related Documents.

Western Union next argues that the Commission may not use its process to obtain access to documents that are subject to confidentiality restrictions imposed by an Arizona state court. Citing the state court's observations that the Monitor materials would not exist but for the settlement agreement and that the confidentiality protections were a material inducement for Western Union to settle, Western Union contends that the Commission has failed to establish its entitlement to these confidential and sensitive materials.[44] We are not persuaded.

First, the confidentiality provisions of the Arizona settlement documents do not by their terms limit the Commission's ability to use investigatory process to obtain the Monitor's reports and related information. The settlement documents do not address the question of whether the reports and related documents must be released in response to compulsory process of a federal agency. On the contrary, the Settlement Agreement specifically states that it "does not bind any federal agencies or any other state's authorities."[45] Indeed, the settlement documents state that the Monitor's reports and the

[42] Pet. Ex. A, at 7-8.

[43] *Invention Submission Corp.*, 965 F.2d at 1089; *Carter*, 636 F.2d at 788.

[44] Pet. 15-16.

[45] Pet. Ex. C ¶ 28.

underlying information may be shared in certain circumstances — including with investigative agencies or in furtherance of the Attorney General's duties.[46]

Second, Western Union errs in contending that CIDs represent an improper attempt to circumvent an order of a state court. The September 2012 ruling dealt solely with the Arizona Attorney General's request to share copies of the reports that had been provided to him.[47] Similarly, the January 2013 order dealt solely with the request made by the Monitor, pursuant to the CID addressed to the Monitor, to disclose copies of the reports in the Monitor's custody.[48] Neither the ruling nor the order purports to address the copies of the Monitor's reports that reside in Western Union's own files, or the other materials sought in Specification 2 of the CID addressed to Western Union – which includes materials besides the Monitor's reports, such as "information Western Union provided to the Monitor" and Western Union's internal reactions to the Monitor's reports.[49] The state court's ruling and order, by their own terms, are simply inapplicable to the documents that Western Union seeks to shield from disclosure.

---

[46] For example, the Monitor is required to "take appropriate steps to maintain the confidentiality of any information entrusted to him or her" and to "share such information only with the State, *appropriate investigative agencies*, and individuals or entities hired by him or her." Pet. Ex. B ¶ 36 (emphasis added). For its part, the office of the Arizona Attorney General must "maintain the confidentiality of any materials or information provided by Western Union under this paragraph and shall not provide such material or information to any third party, except to the extent that disclosure is required by law, otherwise authorized by this Agreement, or *is in the proper discharge of or otherwise furthers the State's official duties and responsibilities*." *Id.*, Ex. C ¶ 17.1.4 (emphasis added). With respect to the reports themselves, the Arizona Attorney General is required to maintain their confidentiality "*except to the extent that disclosure may be necessary by the State in connection with the discharge of its official duties*." *Id.*, Ex. B ¶ 37 (emphasis added).

[47] Pet. Exs. E, F.

[48] Pet. Ex. G.

[49] Although the MEL requires the State of Arizona and Western Union to "maintain the confidentiality of all such information provided to them by the Monitor," Pet. Ex. B ¶ 37, there is nothing in the settlement documents or the state court's subsequent ruling or order that restricts Western Union from disclosing its own business records – such as its communications to the Monitor and its internal documents discussing the Monitor's reports and recommendations.

Third, the Arizona state court did not purport to prohibit the Commission from using its process to obtain the reports or related information either from the Monitor or the State of Arizona. On the contrary, on both occasions the court specifically noted that it was not addressing the scope of the Commission's process authority. When ruling on the Arizona Attorney General's request, the state court explained that it was "mak[ing] no comment" on "the extent that the FTC or Homeland Security has a right to secure information that the monitor has or the Attorney General's Office has."[50] Similarly, when ruling on the Monitor's request, the state court recognized that "it has no jurisdiction, and makes no attempt to determine the enforceability of the FTC's CID," and therefore specifically declined to address "whether the FTC has authority to take" the reports and what the Commission "may do with them" thereafter.[51]

Fourth, even if the Arizona state court had intended to prohibit the FTC from obtaining the Monitor's reports and related materials, confidentiality restrictions under state law must give way if they conflict with federal agencies' statutory power to gather evidence. Agencies of the United States may use their compulsory process to obtain documents whose disclosure would otherwise be barred by state statute.[52] Put differently, even when a state legislature has specifically acted to prohibit disclosure of certain information, those state statutes are preempted to the extent they frustrate the federal statutory schemes that entitle federal agencies to "have access to relevant evidence."[53]

---

[50] Pet. Ex. F, at 21.

[51] Pet. Ex. G, at 3-4.

[52] *See, e.g.*, *EEOC v. Ill. Dep't of Emp't Sec.*, 995 F.2d 106, 107 (7th Cir. 1993) (enforcing EEOC subpoena for transcript of unemployment compensation hearing, despite state statute making such proceedings confidential); *United States ex rel. Office of Inspector Gen., U.S. Dep't of Hous. & Urban Dev. v. Phila. Hous. Auth.*, 2011 WL 382765, at *5 (E.D. Pa. Feb. 4, 2011) (enforcing HUD OIG subpoena seeking employees' partial Social Security Numbers, despite state statutes restricting disclosure of sensitive personal information); *United States v. United Network for Organ Sharing*, 2002 WL 1726536, at *1-*2 (N.D. Ill. May 17, 2002) (enforcing HHS OIG subpoena, despite state statute restricting disclosure of peer review documents); *United States ex rel. Agency for Int'l Dev. v. First Nat'l Bank of Md.*, 866 F. Supp. 884, 887 (D. Md. 1994) (enforcing USAID OIG subpoena, despite state statute restricting disclosure of financial documents); *United States v. N.Y. State Dep't of Taxation & Fin.*, 807 F. Supp. 237, 240-43 (N.D.N.Y. 1992) (enforcing DOL OIG subpoena, despite state statute restricting disclosure of tax and wage records); *EEOC v. County of Hennepin*, 623 F. Supp. 29, 32 (D. Minn. 1985) (enforcing EEOC subpoena, despite state statute permitting production of government personnel information only in response to a court order).

[53] *County of Hennepin*, 623 F. Supp. at 32.

The same considerations apply when a state court purports to restrict the Commission's ability to use its investigative process. "'To . . . federal statute and policy, conflicting state law and policy must yield. Constitution, Art. VI, cl. 2.'"[54]

Fifth, the fact that the requested documents were generated as a result of Western Union's settlement with the Arizona Attorney General does not change the analysis. Documents created pursuant to settlement or in reliance on confidentiality protections are not automatically shielded from all disclosure. For example, even in the context of purely private rights, the Third Circuit has recognized that parties' reliance on a confidentiality order is only one of several factors that must be considered when nonparties seek access to confidential settlement materials.[55] The threshold to forestall disclosure of documents submitted to facilitate settlement is even higher when a case involves – as it does here – "a government agency and an alleged series of deceptive trade practices culminating (it is said) in widespread consumer losses," because "[t]hese are patently matters of significant public concern."[56]

Moreover, Western Union's cited cases – *United States v. Bleznak*, 153 F.3d 16 (2d Cir. 1998), and *McCoo v. Denny's Inc.*, 2000 WL 156824 (D. Kan. Feb. 11, 2000) – do not support the proposition that the Commission may not use process to obtain documents that would not exist but for the Arizona settlement agreement. Notably, the persons seeking disclosure in *Bleznak* and *McCoo* were seeking evidence to use in vindicating their purely private rights. By contrast, the Commission is an agency of the United States and seeks materials in connection with its statutory mandate to prevent unfair and deceptive practices in furtherance of the public interest. Furthermore, in both

---

[54] *Liner v. Jafco, Inc.*, 375 U.S. 301, 309 (1964) (quoting *Sola Elec. Co. v. Jefferson Elec. Co.*, 317 U.S. 173, 176 (1942)).

[55] *Pansy v. Borough of Stroudsburg*, 23 F.3d 772, 787-90 (3d Cir. 1994) (noting that parties' reliance "should not be outcome determinative," and instructing courts to also consider factors such as privacy interests, the purpose for which the information is being sought, whether the information is important to public health and safety, whether sharing would promote fairness and efficiency, and whether the case involves issues important to the public); *see also Daines v. Harrison*, 838 F. Supp. 1406, 1408-09 (D. Colo. 1993) (finding that parties' reliance on confidentiality order was "not enough to tip the balance in their favor" in light of competing interests favoring disclosure, such as the public right of access to court records and the involvement of public agencies and public funds); *cf. Palmieri v. New York*, 779 F.2d 861, 864-66 (2d Cir. 1985) (recognizing that orders sealing court records and a settlement agreement could be modified if warranted by "extraordinary circumstances" or "compelling need").

[56] *FTC v. Standard Fin. Mgmt. Corp.*, 830 F.2d 404, 412 (1st Cir. 1987).

cases, the consent decree at issue specifically barred the requested disclosure.[57] As noted above, the Arizona settlement documents specifically contemplate that the Monitor's reports and the underlying information may be shared in certain circumstances, including with investigative agencies or in furtherance of the Attorney General's duties. Thus, the provisions considered in *Bleznak* and *McCoo* are not comparable to the confidentiality provisions at issue here.

Finally, Western Union suggests that the "appropriate procedure" would be for the Commission to appear before the Arizona state court or seek to intervene.[58] However, the Commission is an agency of the United States not subject to the jurisdiction of state courts. A state may not interfere with a valid exercise of federal authority.[59] Thus, there is no basis for the contention that the Commission must appear before a state tribunal or seek to intervene in a state proceeding to use its statutory process authority to obtain the requested documents – a principle the Arizona court recognized implicitly when it held that "it has no jurisdiction, and makes no attempt to determine the enforceability of the FTC's CID."[60]

2. The FTC May Obtain Western Union's Worldwide Complaints.

Specification 1 of the CID requires Western Union to produce "[a]ll documents referring or relating to complaints made to Western Union by consumers anywhere in the world, referring or relating to fraud-induced money transfers."[61] Under the governing

[57] The intervenors in *Bleznak*, who were parties in a separate private action against the defendants, sought to circumvent specific language in the consent decree that the tapes created pursuant to the settlement would not be "subject to civil process" or "admissible in evidence in civil proceedings." 153 F.3d at 19. Similarly, the *McCoo* plaintiffs were using discovery to seek the materials at issue, an act specifically prohibited by the consent decree provisions barring the Monitor and the parties from disclosing "Confidential Information to any person who is not a party to this Decree, including without limitation any person who seeks such Confidential Information in other litigation through discovery process in other courts." 2000 WL 156824, at *2.

[58] Pet. 16.

[59] *See Goodyear Atomic Corp. v. Miller*, 486 U.S. 174, 180 n.1 (1988) (Supremacy Clause "immunizes the activities of the Federal Government from state interference"); *Mayo v. United States*, 319 U.S. 441, 445 (1943) ("[T]he activities of the Federal Government are free from regulation by any state.").

[60] Pet. Ex. G, at 3.

[61] Pet. Ex. A, at 7 (Specification III.1).

law, this specification must be enforced if the inquiry is within the authority of the agency, the demand is not too indefinite, and the information sought is reasonably relevant to the purpose of the inquiry, as set forth in the Commission's investigatory resolution.

Western Union does not claim that the specification is too indefinite or not reasonably relevant. It contends, however, that the Commission has exceeded its authority in requesting information about transactions that occurred outside the U.S. and further, that the request cannot be reconciled with foreign data privacy laws. We are not persuaded by either of these claims.

The FTC is authorized to obtain through compulsory process Western Union's worldwide complaints about fraud-induced money transfers. In 2006, Congress passed the U.S. SAFE WEB Act, which enhanced the FTC's ability to protect U.S. consumers from perpetrators of fraud operating abroad and to prevent the U.S. from becoming a haven for fraudulent activity targeting foreign victims by amending Section 5's core provisions to confirm the agency's cross-border jurisdictional authority. The SAFE WEB amendments provide that the term "unfair or deceptive acts or practices" in Section 5(a) of the FTC Act "includes such acts or practices involving foreign commerce" that either: "(i) cause or are likely to cause reasonably foreseeable injury within the United States; or (ii) involve material conduct occurring within the United States." 15 U.S.C. § 45(a)(4)(A).

Indeed, the Senate Report on the U.S. SAFE WEB Act cited by Western Union makes it clear that Congress intended to empower the FTC to combat cross-border fraud by obtaining and sharing information from foreign jurisdictions. The report states that the Act will

> authorize the FTC to: (1) share information involving cross-border fraud with foreign consumer protection agencies; (2) secure confidential information from those foreign consumer protection agencies; (3) take fraud-based legal action in foreign jurisdictions; (4) seek redress on behalf of foreign consumers victimized by United States-based wrongdoers; (5) make criminal referrals for cross-border criminal activity; [and] (5) strengthen its relationship with foreign consumer protection agencies.[62]

For this reason, Western Union's reliance on the Supreme Court's decision in *Morrison v. National Australia Bank Ltd.*, 130 S. Ct. 2869 (2010), is misplaced. In *Morrison,* the Supreme Court held, in the context of a private class action involving foreign buyers and sellers operating on foreign security exchanges, that there was no

[62] S. Rep. No. 109-219, at 3 (2006).

"affirmative indication" that Section 10(b) of the SEC Act applies extraterritorially. The "presumption against extraterritoriality" affirmed in *Morrison* does not apply to the FTC's CID here, given Congress' express intent in extending the FTC Act to specified acts and practices involving foreign commerce. *See* 15 U.S.C. § 45(a)(4).

Further, the request in the CID for Western Union's worldwide complaints is proper under both the "material conduct" and "cause or likely to cause reasonably foreseeable injury" tests in Section 45(a)(4).

For one, the FTC's investigation has focused primarily on whether Western Union has adopted and implemented policies and procedures that are sufficient to prevent or limit wrongdoers from using its money transfer system to perpetrate fraud. The "material conduct" at issue is therefore Western Union's actions in developing and administering its antifraud program – activities that Western Union does not dispute occur within the United States.[63] Any complaints from foreign consumers related to fraud-induced money transfers in non-U.S. jurisdictions certainly "involve" this "material conduct" and call into question the effectiveness of these policies and procedures to protect U.S. and non-U.S. consumers alike.[64] The FTC is entitled to such worldwide complaints to help it assess the levels of fraud perpetrated through Western Union's network, the extent of Western Union's knowledge of the number of any fraud-induced money transfers being picked up at particular agent locations, and the adequacy of Western Union's actions in response to

---

[63] Western Union asserts that its oversight of its antifraud program cannot be "material conduct" because it is an "act of omission" involving an alleged failure to act. Pet. 11. This argument ignores the affirmative duty imposed by the BSA on Western Union to implement an AML program. *See* II.C., *supra*. It also ignores the detailed information Western Union already provided the Commission that describes its antifraud program, including program documentation. This information confirms that, far from performing an "act of omission," Western Union affirmatively sets policy and dictates procedures within the U.S. that are designed to detect and curtail fraudulent activities both within and outside the U.S. Western Union also employs procedures developed here to receive complaints, analyze complaint data, and to take remedial action in response to that data. *See generally* Anti-Fraud Program 5-24, 29-33. In further support, we note that the complaints sought by the CID are maintained in the United States.

[64] We note that Western Union does not address the fact that documents responsive to Specification 1 include any complaints by non-U.S. consumers about fraudulent transactions picked up in the U.S. Such complaints, which the company has also refused to provide, directly touch the U.S., and none of the arguments advanced by Western Union calls into question the Commission's authority to use its investigative process to require the company to produce them.

such complaints.[65]

For similar reasons, any failure by Western Union to take effective remedial action against a problematic foreign agent would necessarily cause or be likely to cause reasonably foreseeable injury to consumers within the U.S. As explained above, if Western Union, through complaints it receives from U.S. and foreign victims, or even from foreign victims alone, is able to identify a problem agent abroad, then it may need to take immediate action to suspend or terminate that agent from its system to prevent additional consumers from being victimized. Any future victims may include both U.S. and foreign consumers, because a problem agent in a foreign jurisdiction that is receiving fraud-induced transactions from foreign victims may also likely be receiving fraud-induced transactions from U.S. victims.

Western Union's assertions on this issue fail to account for the worldwide nature of the networks that may be perpetrating fraud through its system. As we have learned, funds transferred by a single consumer victim may subsequently be transferred multiple times through a money transfer network before the funds reach the ultimate perpetrator of the scheme. For example, a U.S. consumer who is the victim of a lottery scheme could transfer funds to a money transfer outlet in Canada, which, in turn, may transfer the funds to another outlet in Romania. The transfer from Canada to Romania injures the U.S. consumer, because it was her funds that were transferred. Similarly, the funds transferred by consumer victims in the U.K. that are picked up in Romania may subsequently be transferred to a con artist operating in the U.S. The fact that the complained-of transfer might have been routed through an agent in Romania, rather than directly to the U.S., would not negate the effects of such a transfer on the U.S.[66]

---

[65] Western Union's claim that fraud is somehow being conducted "unbeknownst" to the company by foreign con artists is troubling and serves to underscore the need for staff to investigate. Pet. 12. The FTC and other law enforcers have put the company on notice that the perpetrators of fraudulent or deceptive practices may be using its money transfer services, and the company has acknowledged and committed to improving its processes for detecting such activities. Indeed, Western Union has a legal obligation to detect and report such unlawful conduct. If Western Union now claims that it is unaware of this fraud, this highlights a need to examine the antifraud program more closely and its ability to detect such conduct.

[66] Though Western Union does not address it, Section 5(a)(4)(B) of the FTC Act, which addresses remedies for U.S. and foreign victims of consumer frauds, also supports the CID's request for worldwide complaints. If Western Union's failure to take reasonable steps to detect and prevent con artists from using its money transfer system causes harm to U.S. and foreign victims, the FTC is empowered by the SAFE WEB Act to remedy this harm. Any complaints from worldwide victims could bear on the scope of

Western Union's references to the need to promote international comity and avoid conflicts among data protection laws do not provide any basis for quashing the CID. Western Union has not cited any actual foreign data protection law, or described how such law would preclude Western Union from providing the FTC with any worldwide complaints.

Furthermore, Western Union's reliance on *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Ct.*, 482 U.S. 522, 546 (1987), is misplaced. First, *Aerospatiale* involved private interests, not a federal agency's use of compulsory process in a law enforcement investigation. Second, contrary to Western Union's assertion, nothing in *Aerospatiale* stands for the proposition that discovery rules "ought never to be construed to violate the law of nations if any other possible construction remains . . . ." [67] Instead, the Supreme Court concluded that the litigants were not required to use the procedures of the Hague Convention to obtain documents maintained outside the United States -- even from foreign corporations.[68] Indeed, federal courts analyzing the *Aerospatiale* decision have often applied the factors described there to order compliance with U.S. discovery requests even in the face of a foreign blocking or other statute.[69]

---

the harm and the proper amount of restitution.

[67] Pet. 12-13 (quoting *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Ct.*, 482 U.S. 522, 546 (1987)). The text quoted by Western Union actually appears in a much older case, *Murray v. Schooner Charming Betsy*, 6 U.S. (2 Cranch) 64, 118 (1804), and was intended to promote international comity as was the Court's decision in *Aerospatiale*. But the *Aerospatiale* Court also explicitly recognized the interests of the United States as an important factor in developing a comity analysis, following the *Charming Betsy* canon, that balances respect for other countries' judicial sovereignty against U.S. discovery requirements.

[68] 482 U.S. at 538-43. The Court explained that foreign blocking statutes

> do not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that statute. Nor can the enactment of such a statute by a foreign nation require American courts to engraft a rule of first resort onto the Hague Convention, or otherwise to provide the nationals of such a country with a preferred status in our courts.

Id. at 544 n. 29 (citations omitted, citing *Societe Internationale Pour Participations Industrielles et Commerciales, S.A. v. Rogers*, 357 U.S. 197, 204-206 (1958)).

[69] *See, e.g.*, *Devon Robotics v. Deviedma*, No. 09-cv-3522, 2010 U.S. Dist. LEXIS

Finally, Western Union fails to cogently explain how the CID undermines the FTC's role in enforcing the U.S.-EU Safe Harbor Framework.[70] Generally, the European Union's Directive on Data Protection requires that transfers of personal data take place only to non-EU countries that provide an "adequate" level of protection. The Framework is deemed adequate and provides a "safe harbor" to receive personal data from the European Union for those U.S. organizations that pledge to comply with a defined set of privacy principles and certify to that commitment.[71] The FTC then enforces that commitment and certification under Section 5 of the FTC Act. Contrary to what Western Union's brief appears to suggest,[72] the FTC has not brought cases for violations of EU data protection laws.[73] Instead, the FTC may treat false certifications of compliance with the Framework as deceptive acts or practices.[74] As the European Commission itself has recognized, "U.S. law will apply to questions of interpretation and compliance with the Safe Harbor principles."[75] The Safe Harbor framework is clear that in the event of a

---

108573, *10-*17 (E.D. Pa. Oct. 8, 2010) (ordering disclosure notwithstanding an Italian blocking statute); *Accessdata Corp. v. Alste Techn*, No. 2:08-cv-569, 2010 U.S. Dist. LEXIS 4566, *4-*8 (D. Utah. Jan. 21, 2010) (ordering disclosure notwithstanding a German blocking statute). This is particularly true in cases involving the enforcement of U.S. law. *See, e.g., In re Air Cargo Shipping Services Antitrust Litigation*, 278 F.R.D. 51, 52-54 (E.D.N.Y. 2010) (finding that "strong national interest[]" in U.S. enforcing antitrust laws outweighed France's interest in controlling access to information within its borders).

[70] Pet. at 13.

[71] *See* Export.gov, U.S.-E.U. Safe Harbor Overview, http://export.gov/safeharbor/eu/eg_main_018476.asp (last updated Apr. 26, 2012). As stated in that overview, "the Principles were solely designed to [deem the Framework to be adequate and] … cannot be used as a substitute for national provisions implementing the Directive that apply to the processing of personal data in the Member States."

[72] Pet. 13.

[73] The cases referenced by Western Union all involved allegations that companies falsely self-certified that they met the Safe Harbor requirements.

[74] *See, e.g., In re Facebook, Inc.*, FTC File No. 092 3184 (July 27, 2012).

[75] *See* Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, at Annex 1 (attaching U.S. Department of Commerce

conflict between U.S. law and the law of another jurisdiction, U.S. companies must still follow U.S. law. The Safe Harbor Framework itself provides that "where U.S. law imposes a conflicting obligation, U.S. organizations whether in the safe harbor or not must comply with the law."[76]

IV. CONCLUSION

For the foregoing reasons, **IT IS HEREBY ORDERED THAT** the Petition of Western Union to Quash Civil Investigative Demands be, and it hereby is, **DENIED**.

IT IS FURTHER ORDERED THAT all responses to the specifications in the Civil Investigative Demand to Western Union must now be produced on or before March 18, 2013.

By the Commission, Commissioner Leibowitz not participating.

Richard C. Donohue
Acting Secretary

Safe Harbor Privacy Principles (July 21, 2000)), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:en:NOT.

[76] *See* Export.gov, Damages for Breaches of Privacy, Legal Authorizations and Mergers and Takeovers in U.S. Law, at § B, http://export.gov/safeharbor/eu/eg_main_018482.asp (last updated Jan. 30, 2009). We note that Western Union is not presently among the organizations that have certified their compliance with the Safe Harbor privacy requirements. *See* http://safeharbor.export.gov/list.aspx (last visited March 4, 2013).