

EXHIBIT 26



**14. CONVENTION ON THE SERVICE ABROAD OF
JUDICIAL AND EXTRAJUDICIAL DOCUMENTS
IN CIVIL OR COMMERCIAL MATTERS¹**

(Concluded 15 November 1965)

The States signatory to the present Convention,
Desiring to create appropriate means to ensure that judicial and extrajudicial documents to be served abroad shall be brought to the notice of the addressee in sufficient time,
Desiring to improve the organisation of mutual judicial assistance for that purpose by simplifying and expediting the procedure,
Have resolved to conclude a Convention to this effect and have agreed upon the following provisions:

Article 1

The present Convention shall apply in all cases, in civil or commercial matters, where there is occasion to transmit a judicial or extrajudicial document for service abroad.
This Convention shall not apply where the address of the person to be served with the document is not known.

CHAPTER I – JUDICIAL DOCUMENTS

Article 2

Each Contracting State shall designate a Central Authority which will undertake to receive requests for service coming from other Contracting States and to proceed in conformity with the provisions of Articles 3 to 6.
Each State shall organise the Central Authority in conformity with its own law.

Article 3

The authority or judicial officer competent under the law of the State in which the documents originate shall forward to the Central Authority of the State addressed a request conforming to the model annexed to the present Convention, without any requirement of legalisation or other equivalent formality.
The document to be served or a copy thereof shall be annexed to the request. The request and the document shall both be furnished in duplicate.

Article 4

If the Central Authority considers that the request does not comply with the provisions of the present Convention it shall promptly inform the applicant and specify its objections to the request.

¹ This Convention, including related materials, is accessible on the website of the Hague Conference on Private International Law (www.hcch.net), under "Conventions" or under the "Service Section". For the full history of the Convention, see Hague Conference on Private International Law, *Actes et documents de la Dixième session (1964)*, Tome III, *Notification* (391 pp.).

Article 5

The Central Authority of the State addressed shall itself serve the document or shall arrange to have it served by an appropriate agency, either –

- a) by a method prescribed by its internal law for the service of documents in domestic actions upon persons who are within its territory, or
- b) by a particular method requested by the applicant, unless such a method is incompatible with the law of the State addressed.

Subject to sub-paragraph (b) of the first paragraph of this Article, the document may always be served by delivery to an addressee who accepts it voluntarily.

If the document is to be served under the first paragraph above, the Central Authority may require the document to be written in, or translated into, the official language or one of the official languages of the State addressed.

That part of the request, in the form attached to the present Convention, which contains a summary of the document to be served, shall be served with the document.

Article 6

The Central Authority of the State addressed or any authority which it may have designated for that purpose, shall complete a certificate in the form of the model annexed to the present Convention.

The certificate shall state that the document has been served and shall include the method, the place and the date of service and the person to whom the document was delivered. If the document has not been served, the certificate shall set out the reasons which have prevented service.

The applicant may require that a certificate not completed by a Central Authority or by a judicial authority shall be countersigned by one of these authorities.

The certificate shall be forwarded directly to the applicant.

Article 7

The standard terms in the model annexed to the present Convention shall in all cases be written either in French or in English. They may also be written in the official language, or in one of the official languages, of the State in which the documents originate.

The corresponding blanks shall be completed either in the language of the State addressed or in French or in English.

Article 8

Each Contracting State shall be free to effect service of judicial documents upon persons abroad, without application of any compulsion, directly through its diplomatic or consular agents.

Any State may declare that it is opposed to such service within its territory, unless the document is to be served upon a national of the State in which the documents originate.

Article 9

Each Contracting State shall be free, in addition, to use consular channels to forward documents, for the purpose of service, to those authorities of another Contracting State which are designated by the latter for this purpose.

Each Contracting State may, if exceptional circumstances so require, use diplomatic channels for the same purpose.

Article 10

Provided the State of destination does not object, the present Convention shall not interfere with –

- a) the freedom to send judicial documents, by postal channels, directly to persons abroad,

- b) the freedom of judicial officers, officials or other competent persons of the State of origin to effect service of judicial documents directly through the judicial officers, officials or other competent persons of the State of destination,
- c) the freedom of any person interested in a judicial proceeding to effect service of judicial documents directly through the judicial officers, officials or other competent persons of the State of destination.

Article 11

The present Convention shall not prevent two or more Contracting States from agreeing to permit, for the purpose of service of judicial documents, channels of transmission other than those provided for in the preceding Articles and, in particular, direct communication between their respective authorities.

Article 12

The service of judicial documents coming from a Contracting State shall not give rise to any payment or reimbursement of taxes or costs for the services rendered by the State addressed.

The applicant shall pay or reimburse the costs occasioned by —

- a) the employment of a judicial officer or of a person competent under the law of the State of destination,
- b) the use of a particular method of service.

Article 13

Where a request for service complies with the terms of the present Convention, the State addressed may refuse to comply therewith only if it deems that compliance would infringe its sovereignty or security.

It may not refuse to comply solely on the ground that, under its internal law, it claims exclusive jurisdiction over the subject-matter of the action or that its internal law would not permit the action upon which the application is based.

The Central Authority shall, in case of refusal, promptly inform the applicant and state the reasons for the refusal.

Article 14

Difficulties which may arise in connection with the transmission of judicial documents for service shall be settled through diplomatic channels.

Article 15

Where a writ of summons or an equivalent document had to be transmitted abroad for the purpose of service, under the provisions of the present Convention, and the defendant has not appeared, judgment shall not be given until it is established that —

- a) the document was served by a method prescribed by the internal law of the State addressed for the service of documents in domestic actions upon persons who are within its territory, or
- b) the document was actually delivered to the defendant or to his residence by another method provided for by this Convention, and that in either of these cases the service or the delivery was effected in sufficient time to enable the defendant to defend.

Each Contracting State shall be free to declare that the judge, notwithstanding the provisions of the first paragraph of this Article, may give judgment even if no certificate of service or delivery has been received, if all the following conditions are fulfilled —

- a) the document was transmitted by one of the methods provided for in this Convention,
- b) a period of time of not less than six months, considered adequate by the judge in the particular case, has elapsed since the date of the transmission of the document,
- c) no certificate of any kind has been received, even though every reasonable effort has been made to obtain it through the competent authorities of the State addressed.

Notwithstanding the provisions of the preceding paragraphs the judge may order, in case of urgency, any provisional or protective measures.

Article 16

When a writ of summons or an equivalent document had to be transmitted abroad for the purpose of service, under the provisions of the present Convention, and a judgment has been entered against a defendant who has not appeared, the judge shall have the power to relieve the defendant from the effects of the expiration of the time for appeal from the judgment if the following conditions are fulfilled –

- a) the defendant, without any fault on his part, did not have knowledge of the document in sufficient time to defend, or knowledge of the judgment in sufficient time to appeal, and
- b) the defendant has disclosed a *prima facie* defence to the action on the merits.

An application for relief may be filed only within a reasonable time after the defendant has knowledge of the judgment.

Each Contracting State may declare that the application will not be entertained if it is filed after the expiration of a time to be stated in the declaration, but which shall in no case be less than one year following the date of the judgment.

This Article shall not apply to judgments concerning status or capacity of persons.

CHAPTER II – EXTRAJUDICIAL DOCUMENTS

Article 17

Extrajudicial documents emanating from authorities and judicial officers of a Contracting State may be transmitted for the purpose of service in another Contracting State by the methods and under the provisions of the present Convention.

CHAPTER III – GENERAL CLAUSES

Article 18

Each Contracting State may designate other authorities in addition to the Central Authority and shall determine the extent of their competence.

The applicant shall, however, in all cases, have the right to address a request directly to the Central Authority.

Federal States shall be free to designate more than one Central Authority.

Article 19

To the extent that the internal law of a Contracting State permits methods of transmission, other than those provided for in the preceding Articles, of documents coming from abroad, for service within its territory, the present Convention shall not affect such provisions.

Article 20

The present Convention shall not prevent an agreement between any two or more Contracting States to dispense with –

- a) the necessity for duplicate copies of transmitted documents as required by the second paragraph of Article 3,
- b) the language requirements of the third paragraph of Article 5 and Article 7,
- c) the provisions of the fourth paragraph of Article 5,
- d) the provisions of the second paragraph of Article 12.

Article 21

Each Contracting State shall, at the time of the deposit of its instrument of ratification or accession, or at a later date, inform the Ministry of Foreign Affairs of the Netherlands of the following –

- a) the designation of authorities, pursuant to Articles 2 and 18,
- b) the designation of the authority competent to complete the certificate pursuant to Article 6,
- c) the designation of the authority competent to receive documents transmitted by consular channels, pursuant to Article 9.

Each Contracting State shall similarly inform the Ministry, where appropriate, of –

- a) opposition to the use of methods of transmission pursuant to Articles 8 and 10,
- b) declarations pursuant to the second paragraph of Article 15 and the third paragraph of Article 16,
- c) all modifications of the above designations, oppositions and declarations.

Article 22

Where Parties to the present Convention are also Parties to one or both of the Conventions on civil procedure signed at The Hague on 17th July 1905, and on 1st March 1954, this Convention shall replace as between them Articles 1 to 7 of the earlier Conventions.

Article 23

The present Convention shall not affect the application of Article 23 of the Convention on civil procedure signed at The Hague on 17th July 1905, or of Article 24 of the Convention on civil procedure signed at The Hague on 1st March 1954.

These Articles shall, however, apply only if methods of communication, identical to those provided for in these Conventions, are used.

Article 24

Supplementary agreements between Parties to the Conventions of 1905 and 1954 shall be considered as equally applicable to the present Convention, unless the Parties have otherwise agreed.

Article 25

Without prejudice to the provisions of Articles 22 and 24, the present Convention shall not derogate from Conventions containing provisions on the matters governed by this Convention to which the Contracting States are, or shall become, Parties.

Article 26

The present Convention shall be open for signature by the States represented at the Tenth Session of the Hague Conference on Private International Law.

It shall be ratified, and the instruments of ratification shall be deposited with the Ministry of Foreign Affairs of the Netherlands.

Article 27

The present Convention shall enter into force on the sixtieth day after the deposit of the third instrument of ratification referred to in the second paragraph of Article 26.

The Convention shall enter into force for each signatory State which ratifies subsequently on the sixtieth day after the deposit of its instrument of ratification.

Article 28

Any State not represented at the Tenth Session of the Hague Conference on Private International Law may accede to the present Convention after it has entered into force in accordance with the first paragraph of Article 27. The instrument of accession shall be deposited with the Ministry of Foreign Affairs of the Netherlands.

The Convention shall enter into force for such a State in the absence of any objection from a State, which has ratified the Convention before such deposit, notified to the Ministry of Foreign Affairs of the Netherlands within a period of six months after the date on which the said Ministry has notified it of such accession.

In the absence of any such objection, the Convention shall enter into force for the acceding State on the first day of the month following the expiration of the last of the periods referred to in the preceding paragraph.

Article 29

Any State may, at the time of signature, ratification or accession, declare that the present Convention shall extend to all the territories for the international relations of which it is responsible, or to one or more of them. Such a declaration shall take effect on the date of entry into force of the Convention for the State concerned.

At any time thereafter, such extensions shall be notified to the Ministry of Foreign Affairs of the Netherlands.

The Convention shall enter into force for the territories mentioned in such an extension on the sixtieth day after the notification referred to in the preceding paragraph.

Article 30

The present Convention shall remain in force for five years from the date of its entry into force in accordance with the first paragraph of Article 27, even for States which have ratified it or acceded to it subsequently.

If there has been no denunciation, it shall be renewed tacitly every five years.

Any denunciation shall be notified to the Ministry of Foreign Affairs of the Netherlands at least six months before the end of the five year period.

It may be limited to certain of the territories to which the Convention applies.

The denunciation shall have effect only as regards the State which has notified it. The Convention shall remain in force for the other Contracting States.

Article 31

The Ministry of Foreign Affairs of the Netherlands shall give notice to the States referred to in Article 26, and to the States which have acceded in accordance with Article 28, of the following –

- a) the signatures and ratifications referred to in Article 26;
- b) the date on which the present Convention enters into force in accordance with the first paragraph of Article 27;
- c) the accessions referred to in Article 28 and the dates on which they take effect;
- d) the extensions referred to in Article 29 and the dates on which they take effect;
- e) the designations, oppositions and declarations referred to in Article 21;
- f) the denunciations referred to in the third paragraph of Article 30.

In witness whereof the undersigned, being duly authorised thereto, have signed the present Convention.

Done at The Hague, on the 15th day of November, 1965, in the English and French languages, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Government of the Netherlands, and of which a certified copy shall be sent, through the diplomatic channel, to each of the States represented at the Tenth Session of the Hague Conference on Private International Law.

EXHIBIT 27

Status table

14: Convention of 15 November 1965 on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters

Entry into force: 10-II-1969

Last update: 4-VI-2014

Number of Contracting States to this Convention: 68

 [View and/or print full status report](#)

1) S = Signature

2) R/A/Su = Ratification, Accession or Succession

3) Type = R: Ratification or Approval;

A: Accession;

A*: Accession giving rise to an acceptance procedure; click on A* for details of acceptances of the accession;

C: Continuation;

Su: Succession;

Den: Denunciation;

4) EIF = Entry into force

5) Ext = Extensions of application

6) Auth = Designation of Authorities

7) Res/D/N = Reservations, declarations or notifications

Members of the Organisation ([click here for the non-Member States](#))

States	S ¹	R/A/Su ²	Type ³	EIF ⁴	Ext ⁵	Auth ⁶	Res/D/N ⁷
Albania		1-XI-2006	A	1-VII-2007		3	
Argentina		2-II-2001	A	1-XII-2001		2	D,Res 5,10,15,16
Australia		15-III-2010	A	1-XI-2010	7	5	D 5,8,9,10,15,16,17,29
Belarus		6-VI-1997	A	1-II-1998		1	
Belgium	21-I-1966	19-XI-1970	R	18-I-1971		2	D 8,15,16

States	S ¹	R/A/Su ²	Type ³	EIF ⁴	Ext ⁵	Auth ⁶	Res/D/N ⁷
Bosnia and Herzegovina		16-VI-2008	A	1-II-2009		1	
Bulgaria		23-XI-1999	A	1-VIII-2000		3	D 5,8,10,15,16
Canada		26-IX-1988	A	1-V-1989		4	D 5,8,10,11,12,15,16,2
China, People's Republic of		6-V-1991	A	1-I-1992		8	D,N 5,8,10,15,16
Croatia		28-II-2006	A	1-XI-2006		3	Res,D 5,6,8,9,10,15,16
Cyprus		26-X-1982	A	1-VI-1983		4	D 8,10,15,16
Czech Republic		28-I-1993	Su	1-I-1993		4	D,Res 8,10,15,29
Denmark	7-I-1969	2-VIII-1969	R	1-X-1969		3	D 10,15,16
Egypt	1-III-1966	12-XII-1968	R	10-II-1969		1	Res 8,10
Estonia		2-II-1996	A	1-X-1996		1	D 10,15,16
Finland	15-XI-1965	11-IX-1969	R	10-XI-1969		2	D 2,9,10
France	12-I-1967	3-VII-1972	R	1-IX-1972	1	3	D 8,15,16
Germany	15-XI-1965	27-IV-1979	R	26-VI-1979		3	D 5,8,10,15,16
Greece	20-VII-1983	20-VII-1983	R	18-IX-1983		1	D 8,10,15
Hungary		13-VII-2004	A	1-IV-2005		3	D 2,5,6,8,9,10,15,16
Iceland		10-XI-2008	A	1-VII-2009		1	D,Res 10,15,16
India		23-XI-2006	A	1-VIII-2007		1	D,Res 8,10,15,16
Ireland	20-X-1989	5-IV-1994	R	4-VI-1994		3	D,Res 10,15
Israel	25-XI-1965	14-VIII-1972	R	13-X-1972		2	D,Res 10,16
Italy	25-I-1979	25-XI-1981	R	24-I-1982		3	D 5,12

States	S ¹	R/A/Su ²	Type ³	EIF ⁴	Ext ⁵	Auth ⁶	Res/D/N ⁷
Japan	12-III-1970	28-V-1970	R	27-VII-1970		3	D 10,15
Korea, Republic of		13-I-2000	A	1-VIII-2000		2	D,Res 8,10,15
Latvia		28-III-1995	A	1-XI-1995		4	D 5,8,10,15
Lithuania		2-VIII-2000	A	1-VI-2001		1	D,Res 8,10,15,16
Luxembourg	27-X-1971	9-VII-1975	R	7-IX-1975		1	D,Res 5,8,15,16
Malta		24-II-2011	A	1-X-2011		1	D 8,10
Mexico		2-XI-1999	A	1-VI-2000		2	D 5,6,7,8,10,12,15,16
Monaco		1-III-2007	A	1-XI-2007		2	D 8,10,15,16
Montenegro		16-I-2012	A	1-IX-2012		2	D 8,10,15
Morocco		24-III-2011	A	1-XI-2011		1	
Netherlands	15-XI-1965	3-XI-1975	R	2-I-1976	1	5	D 15,16
Norway	15-X-1968	2-VIII-1969	R	1-X-1969		3	D,Res 8,10,15,16
Poland		13-II-1996	A	1-IX-1996		4	Res 8,10
Portugal	5-VII-1971	27-XII-1973	R	25-II-1974		2	D 8,15,16
Romania		21-VIII-2003	A	1-IV-2004		2	D 8,16
Russian Federation		1-V-2001	A	1-XII-2001		4	D,Res 2,3,5,6,8,9,10,12,15
Serbia		2-VII-2010	A	1-II-2011		2	D 5,6,8,10,15,16
Slovakia		15-III-1993	Su	1-I-1993		4	D 8,10,15,29
Slovenia		18-IX-2000	A	1-VI-2001		1	D,Res 8,10,15,16
Spain	21-X-1976	4-VI-1987	R	3-VIII-1987		3	D 15,16

States	S ¹	R/A/Su ²	Type ³	EIF ⁴	Ext ⁵	Auth ⁶	Res/D/N ⁷
Sri Lanka		31-VIII-2000	A	1-VI-2001		3	D 7,8,10,15
Sweden	4-II-1969	2-VIII-1969	R	1-X-1969		2	D 5,10
Switzerland	21-V-1985	2-XI-1994	R	1-I-1995		3	D,Res 1,5,8,10,15
The former Yugoslav Republic of Macedonia		23-XII-2008	A	1-IX-2009		1	D,Res 5,6,8,9,10,15,16,21
Turkey	11-VI-1968	28-II-1972	R	28-IV-1972		3	Res,D 8,10,15,16
Ukraine		1-II-2001	A	1-XII-2001		3	D,Res 8,10,15,16
United Kingdom of Great Britain and Northern Ireland	10-XII-1965	17-XI-1967	R	10-II-1969	14	4	D 2,5,10,15,16,18
United States of America	15-XI-1965	24-VIII-1967	R	10-II-1969	1	1	D 2,15,16,29
Venezuela		29-X-1993	A	1-VII-1994		1	D,Res 5,8,10,15,16

Non-Member States of the Organisation ([click here for the Members](#))

States	S ¹	R/A/Su ²	Type ³	EIF ⁴	Ext ⁵	Auth ⁶	Res/D/N ⁷
Antigua and Barbuda		1-V-1985	Su	1-XI-1981		1	
Armenia		27-VI-2012	A	1-II-2013			
Bahamas		17-VI-1997	A	1-II-1998		1	
Barbados		10-II-1969	A	1-X-1969		1	
Belize		8-IX-2009	A	1-V-2010			
Botswana		10-II-1969	A	1-IX-1969		3	D 5,10,15
Colombia		10-IV-2013	A	1-XI-2013		1	
Kuwait		8-V-2002	A	1-XII-2002		3	D,Res 6,8,9,10,15,16,18
Malawi		24-IV-1972	A	1-XII-1972		1	

States	S ¹	R/A/Su ²	Type ³	EIF ⁴	Ext ⁵	Auth ⁶	Res/D/N ⁷
Pakistan		7-XII-1988	A	1-VIII-1989		3	D 8,15,16
Republic of Moldova		4-VII-2012	A	1-II-2013		1	D,Res 5,8,15,16
Saint Vincent and the Grenadines		6-I-2005	Su	27-X-1979		3	D 5,10,15
San Marino		15-IV-2002	A	1-XI-2002		3	D 8,10,15
Seychelles		18-XI-1980	A	1-VII-1981		1	D 8,10,15,16

1) S = Signature

2) R/A/Su = Ratification, Accession or Succession

3) Type = R: Ratification or Approval;

A: Accession;

A*: Accession giving rise to an acceptance procedure; click on A* for details of acceptances of the accession;

C: Continuation;

Su: Succession;

Den: Denunciation;

4) EIF = Entry into force

5) Ext = Extensions of application

6) Auth = Designation of Authorities

7) Res/D/N = Reservations, declarations or notifications

EXHIBIT 28

Authorities

	Kuwait - Central Authority & practical information	
Address	Central Authority(ies):	
	<i>Ministry of Justice, International Relations Department</i>	
	Contact details:	
	Address:	The State of Kuwait Ministry of Justice International Relations Department Ministries Complex Building No 14 P.O. Box 6 Safaat 13001 Kuwait City
	Telephone:	+965 2248-6367 / 2248 6705
	Fax:	+965 2243-5221 / 2244-2475 / 2244-1390
	E-mail:	mail@moj.gov.kw
	General website:	Ministry of Justice Ministry of Justice - Directory
	Contact person:	
	Languages spoken by staff:	Arabic, English
	Practical Information:	
	<i>(The following information was provided by the relevant State authorities or was obtained from the replies to the 2003 and/or 2008 Service Convention Questionnaires)</i>	
	Forwarding authorities (Art. 3(1)):	Ministry of Justice International Relations Department
	Methods of service (Art. 5(1)(2)):	Service is processed by the Execution Department, which is subordinate to the Ministry of Justice.
	The translation requirements are subject to Article 5 of the Service Convention.	

Translation requirements (Art. 5(3)):	
Costs relating to execution of the request for service (Art. 12):	No charges
Time for execution of request:	One week
Oppositions and declarations (Art. 21(2)):	Click here to read all the declarations made by Kuwait under this Convention
Art. 8(2):	Opposition
Art. 10(a):	Opposition
Art. 10(b):	Opposition
Art. 10(c):	Opposition
Art. 15(2):	No declaration of applicability (see declaration confirming non-applicability)
Art. 16(3):	Declaration
Derogatory channels (bilateral or multilateral agreements or internal law permitting other transmission channels) (Arts. 11, 19, 24 and 25) Disclaimer: <i>Information may not be complete or fully updated – please contact the relevant authorities to verify this information.</i>	Bilateral conventions on judicial co-operation: <i>Bulgaria, Egypt</i> (ratified by law 96/1977); <i>Lebanon; Morocco</i> (ratified by law 43/1998); <i>Tunisia</i> (ratified by law 123/1977); <i>Turkey</i> . A multilateral convention on judicial co-operation was concluded between the States of the Co-operation Council for the Arab States of the Gulf: <i>Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates</i> (ratified by law 44/1998). Co-operation Council for the Arab States of the Gulf www.gcc-sg.org/eng/
Useful links:	

(This page was last updated on 8 November 2010)

Conventions

- [Convention of 15 November 1965 on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters](#) [14]

Declarations Reservations

Articles: 6,8,9,10,15,16,18

[\(Click here for the Central Authority designated by Kuwait and other practical information\)](#)

Text of the declarations:

"(...)

4. The opposition to methods of service of judicial documents mentioned in Article 8 and 10 of the Convention.

5. The reservation against Paragraph 2 of Article 15.

6. The understanding of Paragraph 3 of Article 16 of the Convention, as for the time limit, mentioned in this paragraph, is the time fixed by the law of the trial judge or one year following the date of judgment which ever is longer."

Additional information received 29-VI-2005:

"1. The Central Authority, which shall receive requests for service of documents, sent by the other contracting state, pursuant to Article 2 of the Convention, is the Ministry of Justice (International Relations Department). The State has the right to designate many central authorities, pursuant to Article 18 of the Convention.

2. The Ministry of Justice is the competent authority to complete a certificate, mentioned in Article 6 of the Convention.

3. The competent authority to receive documents mentioned in Article 9 of the Convention is the Ministry of Justice (International Relations Department)."

EXHIBIT 29

Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125) and the common law of trespass to chattels, unjust enrichment and conversion.

2. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125) and constitute trespass to chattels, unjust enrichment and conversion, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. Microsoft owns the registered trademarks “Bing,” “Internet Explorer,” “Microsoft,” and “Windows” used in connection with its services, software and products.

4. There is good cause to believe that, unless the Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants’ ongoing violations. The evidence set forth in Microsoft’s Brief in Support of Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction (“TRO Application”), and the accompanying declarations and exhibits, demonstrates that Microsoft is likely to prevail on its claim that Defendants have engaged in violations of the foregoing law by:

- a. intentionally accessing and sending malicious code to Microsoft’s and its customers’ protected computers and Windows operating systems, without authorization and exceeding authorization, in order to infect those computers and make them part of the computer botnet known as the “ZeroAccess” botnet (the “botnet”);
- b. sending malicious code to configure, deploy and operate a botnet;
- c. taking control of Internet search engine results, including results provided by Microsoft’s Bing search engine, and redirecting clicks on those results to locations different from those intended by Microsoft and its customers, without their authorization or consent;

- d. taking control of Microsoft's Internet Explorer browser and generating clicks through that browser without the authorization or consent of Microsoft or its customers;
- e. creating unauthorized versions and instances of Microsoft's Internet Explorer browser, thereby creating unauthorized copies of Microsoft's Internet Explorer trademark and falsely indicating that such versions and instances of Internet Explorer are associated with or approved by Microsoft, the purpose of which is to deceive customers;
- f. creating unauthorized versions and instances of Microsoft's Bing Search engine web page and functionality, thereby creating unauthorized copies of Microsoft's Bing trademark and falsely indicating that such versions and instances of the Bing search engine are associated with or approved by Microsoft, the purpose of which is to deceive customers;
- g. creating and redirecting Microsoft's customers to websites containing malicious software or unauthorized copies of Microsoft's trademarks, without the authorization or consent of Microsoft or its customers, and falsely indicating that such websites are associated with or approved by Microsoft, the purpose of which is to deceive customers;
- h. collecting personal information without authorization and content, including personal search engine queries and terms; and
- i. delivering malicious code.

5. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft, its customers, and the public. There is good cause to believe that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court;

6. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other

disposition or concealment by Defendants of botnet command and control software that is hosted at and otherwise operates through the Internet Protocol (IP) addresses and Internet domains listed in Appendix A to this Order from the destruction or concealment of other discoverable evidence of Defendants' misconduct available at those locations if Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's TRO Application and accompanying declarations and exhibits, Microsoft is likely to be able to prove that:

- a. Defendants are engaged in activities that directly violate United States law and harms Microsoft, its customers and the public;
- b. Defendants have continued their unlawful conduct despite the clear injury to Microsoft, its customers, and the public;
- c. Defendants are likely to delete or relocate the harmful, malicious and trademark infringing botnet command and control software at issue in Microsoft's TRO Application, which is operating at and disseminated through the IP addresses and domains at issue, and to destroy information and evidence of their misconduct stored at the IP addresses and domains; and
- d. Defendants are likely to warn their associates engaged in such activities if informed of Microsoft's action.

7. Microsoft's request for this emergency *ex parte* relief is not the result of any lack of diligence on Microsoft's part, but instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), 15 U.S.C. § 1116(a) and 28 U.S.C. § 1651(a), good cause and the interest of justice require that this Order be Granted without prior notice to Defendants, and accordingly, Microsoft is relieved of the duty to provide Defendants with prior notice of Microsoft's motion;

8. There is good cause to believe that Defendants have specifically directed their activities to computers of Microsoft's customers located in the Western District of Texas, have engaged in illegal activity using IP addresses identified in Appendix A to this Order that are

registered to command and control servers located at hosting companies in Germany, Latvia, the Netherlands, Switzerland and Luxembourg (set forth in Appendix A), and have engaged in illegal activity by using the domains identified in Appendix A, by directing malicious botnet code and content to said computers of Microsoft's customers. There is good cause to believe that Defendants have directed said malicious botnet code and content through certain instrumentalities – specifically the computer networks of the Internet Service Providers (ISPs) identified in Appendix B to this Order that Microsoft's customers use to access the Internet, and the hosting companies and domain registries identified in Appendix A to this Order.

9. There is good cause to believe that Defendants have engaged in illegal activity by using the networks of the ISPs identified in Appendix B and the hosting facilities and domain registration facilities of the companies in Appendix A, to deliver from the IP Addresses and domains identified in Appendix A, the malicious botnet code and content that Defendants use to maintain and operate the botnets to the computers of Microsoft's' customers.

10. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants must be prohibited from sending malicious botnet code and content from the IP Addresses identified in Appendix A to computers of Microsoft's customers. There is good cause to believe that to immediately halt the injury caused by Defendants, the ISPs identified in Appendix B and the hosting companies identified in Appendix A should take steps to block incoming and/or outgoing traffic on their respective networks that originates or has been sent from and/or to the IP Addresses identified in Appendix A such that said traffic will not reach victim end-user computers on the ISPs' respective networks and/or the computers at the IP Addresses in Appendix A.

11. There is good cause to believe that Defendants have engaged in illegal activity using the IP Addresses identified in Appendix A to host the command and control software and content used to maintain and operate the botnet. There is good cause to believe that in order to immediately halt the injury caused by Defendants and to ensure the future prosecution of this case it not rendered fruitless by attempts to delete, hide, conceal, or otherwise render

inaccessible the software components that create, distribute, and are involved in the creation, perpetuation, and maintenance of the botnet and prevent the creation and distribution of unauthorized copies of Microsoft's registered trademarks and carry out other harmful conduct, with respect to the Defendants' most current, active command and control servers hosted at the IP Addresses, the following actions should be taken. The ISPs identified in Appendix B and the hosting companies identified in Appendix A should block incoming and/or outgoing traffic on their respective networks that originates or has been sent from and/or to the IP Addresses identified in Appendix A, such that said traffic will not reach victim end-user computers on the ISPs' respective networks and/or the computers at the IP Addresses in Appendix A, and should take other reasonable steps to block such traffic to and/or from any other IP addresses to which Defendants may move the botnet infrastructure, identified by Microsoft and which the Court may order to be subject to this Order, to ensure that Defendants cannot use such infrastructure to control the botnet.

12. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains identified in Appendix A to this order to host the command and control software and content used to maintain and operate the botnet. There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' current and prospective domains set forth in Appendix A must be immediately redirected to the Microsoft-secured name-servers named NS1.microsoftinternetsafety.net and NS2.microsoftinternetsafety.net and thus made inaccessible to Defendants.

13. There is good cause to believe that to immediately halt the injury, the execution of this Order should be carried out in a coordinated manner by Microsoft and by the ISPs identified in Appendix B to this Order and the domain registries and hosting companies identified in Appendix A to this Order on or about 10:00 a.m. Central Standard Time on December 5, 2013, or such other date and time within eight days of this order as may be reasonably requested by Microsoft.

14. There is good cause to permit notice of the instant Order, notice of the Preliminary Injunction hearing and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, satisfy Fed. R. Civ. P. 4(f)(3) and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) by personal delivery upon Defendants who provided accurate contact information in the U.S., if any, (2) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided accurate contact information in foreign countries that are signatory to such treaties, if any, (3) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to their hosting companies and as agreed to by Defendants in their hosting agreements, (4) publishing notice on a publicly available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

IT IS THEREFORE ORDERED that, Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from (1) intentionally accessing and sending malicious software or code to Microsoft's and its customers protected computers and Windows operating systems, without authorization, in order to infect those computers and make them part of any botnet, (2) sending malicious code to configure, deploy and operate a botnet, (3) taking control of internet search engine results or browsers, including Microsoft's Bing search engine and Internet Explorer browser, (4) redirecting search engine results or browser activities or generating unauthorized "clicks," (5) collecting personal information including search terms and keywords, (6) configuring, deploying, operating or otherwise participating in or facilitating the botnet described in the TRO Application, including but not limited to the command and control software hosted at and operating through the IP addresses set forth herein and through any other component or element of the botnet in any location, (7) misappropriating that which rightfully belongs to Microsoft or

its customers or in which Microsoft has a proprietary interest or (8) undertaking similar activity that inflicts harm on Microsoft, its customers, or the public.

IT IS FURTHER ORDERED that, Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from (1) using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademarks "Bing," "Internet Explorer," "Microsoft" or "Windows," bearing registration numbers 2872708, 2463526, 2277112 and 3883548, (2) creating unauthorized copies, versions and instances of Microsoft's Internet Explorer browser, Bing search engine, and trademarks or falsely indicating that Microsoft is associated with or approves the foregoing, (3) using in connection with Defendants' activities, products or services any false or deceptive designation, representation or description of Defendants' or of their activities, whether by symbols, words, designs or statements, which would damage or injure Microsoft or give Defendants an unfair competitive advantage or result in deception of consumers, or (4) acting in any other manner which suggests in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Microsoft, or passing off Defendants' activities, products or services as Microsoft's.

IT IS FURTHER ORDERED that, with respect to any the IP Addresses set forth in Appendix A to this Order, the ISPs identified in Appendix B to this Order shall take reasonable best efforts to implement the following actions:

A. Without the need to create logs or other documentation, identify incoming and/or outgoing Internet traffic on their respective networks that originates and/or is being sent from and/or to the IP Addresses identified in Appendix A that is directed to and/or from computers that connect to the Internet through the ISPs' respective networks;

B. Block incoming and/or outgoing Internet traffic on their respective networks that originate and/or are being sent from and/or to the IP Addresses identified in Appendix A that is directed to and/or from computers that connect to the Internet through the ISPs' respective networks;

C. Take other reasonable steps to block such traffic to and/or from any other IP addresses to which Defendants may move the botnet infrastructure, identified by Microsoft and which the Court may order to be subject to this Order, to ensure that Defendants cannot use such infrastructure to control the botnet.

D. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as necessary to communicate with hosting companies or other ISPs to execute this order;

E. Take all reasonable steps necessary to block the IP Addresses in Appendix A, as set forth above, so to prevent Defendants or Defendants' representatives or any other person, from accessing the IP Addresses, except as explicitly provided for in this Order;

F. Not enable, and shall take all reasonable steps to prevent, any circumvention of this order by Defendants, Defendants' representatives or any other person;

G. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order;

IT IS FURTHER ORDERED that, with respect to the IP Addresses in Appendix A, the non-U.S. hosting companies set forth at Appendix A are respectfully requested, but not ordered, to comply with the following steps, in order to protect the integrity and security of the Internet, to protect the hosting companies' own systems, to protect end-user victims of the botnet in all countries, to advance the public interest and to protect Microsoft and its customers from the botnet:

A. Take all reasonable steps necessary to completely block all access to and all traffic to and from the IP Addresses set forth in Appendix A by Defendants, Defendants' representatives, resellers, and any other person or computer, except as explicitly provided for in this Order;

B. Completely disable the computers, servers, electronic data storage devices, software, data or media assigned to or otherwise associated with the IP Addresses set forth in

Appendix A and make them inaccessible from any other computer on the Internet, any internal network, or in any other manner, to Defendants, Defendants' representatives and all other persons, except as otherwise ordered herein;

C. Completely, and until further order of this Court, suspend all services associated with the IP Addresses set forth in Appendix A;

D. Not enable, and shall take all reasonable steps to prevent, any circumvention of this order by Defendants or Defendants' representatives associated with the IP Addresses or any other person;

E. Log all attempts to connect to or communicate with the IP Addresses set forth in Appendix A;

F. Preserve, retain and produce to Microsoft all documents and information sufficient to identify and contact Defendants and Defendants' representatives operating or controlling the IP Addresses set forth in Appendix A, including any and all individual or entity names, mailing addresses, e-mail addresses, facsimile numbers and telephone numbers or similar contact information, including but not limited to such contact information reflected in billing, usage, access and contact records and all records, documents and logs associated with Defendants' or Defendants' Representatives' use of or access to the IP Addresses.

G. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as explicitly provided for in this Order;

H. Transfer any content and software hosted at the IP Addresses listed in Appendix A that are not associated with Defendants, if any, to new IP Addresses not listed in Appendix A; notify any non-party owners of such action and the new IP addresses, and direct them to contact Microsoft's counsel, Gabriel M. Ramsey, Orrick Herrington & Sutcliffe, 1000 Marsh Road, Menlo Park, CA 90425-1015, gramsey@orrick.com, (Tel: 650-614-7400), to facilitate any follow-on action;

I. Provide reasonable assistance in implementing the terms of this Order and take no action to frustrate the implementation of this Order.

IT IS FURTHER ORDERED that, with respect to any *currently registered* domains set forth in Appendix A, the domain registries located in the United States shall take the following actions:

A. Maintain unchanged the WHOIS or similar contact and identifying information as of the time of receipt of this Order and maintain the domains with the current registrar;

B. The domains shall remain active and continue to resolve in the manner set forth in this Order;

C. Prevent transfer or modification of the domains by Defendants or third parties at the registrar;

D. The domains shall be redirected to secure servers by changing the authoritative name servers to NS1.microsoftinternetsafety.net and NS2.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name server or taking other reasonable steps to work with Microsoft to ensure the redirection of the domains and to ensure that Defendants cannot use them to control the botnet.

E. Take all steps required to propagate to the foregoing changes through the DNS, including domain registrars;

F. Preserve all evidence that may be used to identify the Defendants using the domains.

G. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as necessary to communicate with domain registrars and registries to execute this order.

IT IS FURTHER ORDERED that, with respect to any domains set forth in Appendix A that are *currently unregistered*, the domain registries and registrars located in the United States shall take the following actions:

A. Transfer the domains to the control of Microsoft, such that Microsoft is the registrant with control over hosting and administration of the domains. Domains should be transferred to Microsoft's account at the sponsoring registrar MarkMonitor.

B. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following;

Domain Administrator
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
United States
Phone: +1.4258828080
Facsimile: +1.4259367329
domains@microsoft.com

C. The domains shall be made active and shall resolve in the manner set forth in this order or as otherwise specified by Microsoft.

D. The domains shall be assigned the authoritative name servers NS1.microsoftinternetsafety.net and NS2.microsoftinternetsafety.net and, as may be necessary, the IP address associated with name servers or taking such other reasonable steps to work with Microsoft to ensure that the domains and subdomains are put within Microsoft's control, and to ensure that Defendants cannot use them to control the botnet.

E. Refrain from providing any notice or warning to, or communicating in any way with Defendants or Defendants' representatives and refrain from publicizing this Order until this Order is executed in full, except as necessary to communicate with domain registrars or registries to execute this order.

IT IS FURTHER ORDERED that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including (1) by personal delivery upon Defendants who provided accurate contact information in the U.S., if any; (2) personal delivery through the Hague Convention on Service Abroad or similar treaties upon defendants who provided accurate contact information in foreign countries that are signatory to such treaties, if any, (3) transmission by email, facsimile, mail and/or

personal delivery to the contact information provided by Defendants to their hosting companies and as agreed to by Defendants in their hosting agreements, (4) publishing notice on a publicly available Internet website and/or in newspapers in the communities where Defendants are believed to reside.

IT IS FURTHER ORDERED, pursuant to Federal Rule of Civil Procedure 65(b) that the Defendants shall appear before this Court on December ¹², 2013 at ^{9:30 am} to show cause, if there is any, why this Court should not enter a Preliminary Injunction, pending final ruling on the Complaint against the Defendants, enjoining them from the conduct temporarily restrained by the preceding provisions of this Order.

IT IS FURTHER ORDERED that Microsoft shall post bond in the amount of \$250,000 as cash to be paid into the Court registry.

IT IS FURTHER ORDERED that the Defendants shall file with the Court and serve on Microsoft's counsel any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later than two (2) days prior to the hearing on Microsoft's request for a preliminary injunction. Microsoft may file responsive or supplemental pleadings, materials, affidavits, or memoranda with the Court and serve the same on counsel for the Defendants no later than one (1) day prior to the preliminary injunction hearing in this matter. Provided that service shall be performed by personal or overnight delivery, facsimile or electronic mail, and documents shall be delivered so that they shall be received by the other parties no later than 4:00 p.m. (Central Standard Time) on the appropriate dates listed in this paragraph.

IT IS SO ORDERED

Entered this 25th day of November, 2013.


United States District Judge

EXHIBIT 30

between U.S. Internet users and the Fraud Control IP Addresses. Microsoft also engaged with law enforcement agencies in the United States and Europe to apprise them of the TRO and its expected impact on the ZeroAccess botnet infrastructure.

On December 5, 2013 at 10 a.m. central time, blocking of traffic to and from the Fraud Control IP Addresses commenced, per the TRO, and Microsoft observed a dramatic decline in the click fraud and browser hijacking operations of the ZeroAccess botnet. Also on December 5, 2013, Microsoft is informed that European law enforcement agencies undertook surveillance of the Fraud Control IP Addresses before physically seizing the servers associated with the Fraud Control IP Addresses, permanently disconnecting them from the Internet.

Defendants initially pushed an updated configuration file that contained four new Fraud Control IP Addresses, in an attempt to circumvent the TRO. However, Microsoft is informed that European law enforcement immediately responded to those four new IP addresses and to Defendants' attempt to reconstitute the botnet. Shortly thereafter, Defendants pushed another update to the portion of the botnet that they could control that contained a message in the form of the literal text "white flag;" this second update included instructions that caused infected computers to cease all remaining click fraud and browser hijacking activities of the ZeroAccess botnet. As of the date of this filing, the ZeroAccess click fraud and browser hijacking functions have stopped.

On December 11, 2013, Microsoft was contacted by agents with the Federal Bureau of Investigation's Cyber Task Force in Seattle, who informed Microsoft that the Federal Bureau of Investigation has an open criminal matter in the Southern District of New York relating to the ZeroAccess botnet. The Federal Bureau of Investigation requested that Microsoft stand down in its civil matter involving the botnet, to prevent any potential interference with the government's

action.

Given the effectiveness of the TRO, the fact that the known Fraud Control IP Addresses are all disabled, the prominent role European law enforcement agencies have now undertaken to ensure cessation of the ZeroAccess botnet's click fraud and browser hijacking operations, and Microsoft's desire to ensure that its pursuit of civil remedies does not interfere with active law enforcement efforts in the United States and abroad, Microsoft hereby dismisses this action without prejudice pursuant to Federal Rule of Civil Procedure 41(a)(1)(A)(i).

Dated: December 12, 2013

Respectfully submitted,

FISH & RICHARDSON P.C.

By: /s/ William Thomas Jacks

William Thomas Jacks
Texas Bar No. 10452000
jacks@fr.com
David M. Hoffman
Texas Bar No. 24046084
hoffman@fr.com

111 Congress Ave., Suite 810
Austin TX 78701

Telephone: +1-512-472-5070

Facsimile: +1-512-320-8935

Of Counsel:

ORRICK, HERRINGTON & SUTCLIFF LLP

Gabriel M. Ramsey
(*pro hac vice*)
gramsey@orrick.com

Jeffrey L. Cox
(*pro hac vice*)
jcox@orrick.com

Jacob M. Heath
(*pro hac vice*)
jheath@orrick.com

Robert L. Uriarte
(*pro hac vice*)
ruriarte@orrick.com

100 Marsh Road
Menlo Park, CA 94025
Telephone: +1-650-614-7400
Facsimile: +1-650-614-7401

Attorneys for Plaintiff
MICROSOFT CORPORATION

Notice of Dismissal