

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

DONNA HITESHEW, individually and on  
behalf of all others similarly situated,

Plaintiff,

v.

MARRIOTT INTERNATIONAL, INC., a  
Delaware corporation, and STARWOOD  
HOTELS & RESORTS WORLDWIDE,  
LLC, a Maryland limited liability company,

Defendants.

Case No.: 8:18-cv-03755

**Honorable Paul W. Grimm**

**NOTICE REGARDING DEFENDANTS' INTENT TO NOT ENFORCE  
WEBWATCHER ARBITRATION AND CLASS ACTION WAIVER**

Plaintiff Donna Hiteshew by and through her undersigned counsel, Edelson PC, hereby respectfully submits this notice regarding Defendants Marriott International Inc.'s and Starwood Hotels & Resorts Worldwide, LLC's intention to not seek enforcement of the arbitration and class action waiver provisions contained in the so-called WebWatcher terms of service, a third-party web-monitoring service recently offered by Defendants to class members following announcement of their data breach. The purpose of such notice is to ensure that putative class members and the Court are informed of Defendants' stated position and to eliminate the potential confusion to class members resulting from the WebWatcher terms.<sup>1</sup> In support of the instant filing, Plaintiff states as follows:

---

<sup>1</sup> Prior to this filing, Plaintiff's counsel informed Defendants' counsel of the need to alert class members and the Court of Defendants' intention to not enforce the WebWatcher arbitration and class action waiver, and suggested that the Parties do so jointly. (*See* Declaration of Evelyn J. Rapp, attached as Exhibit A, ¶ 5.) Defendants' counsel, however, did not respond. (*Id.*)

1. Like so many others who were affected by Defendants' massive data breach, on December 6, 2018 Plaintiff Donna Hiteshew ("Plaintiff") filed a putative Class Action Complaint against Defendants Marriott International, Inc., and Starwood Hotels & Resorts Worldwide LLC (collectively "Marriott" or "Defendants"), arising from the breach of Marriott's security system that exposed the personal data of approximately 500 million people. (Dkt. 1.)

2. Beyond Defendants lax data security, another issue addressed in Plaintiff's Complaint, was the confusion being created by Defendants in notifying class members of the breach. Namely, Defendants disseminated emails and directed class members to a website, which among other things, advised of the breach and offered customers one-year of WebWatcher, a web monitoring service that is ostensibly intended to aid people in monitoring whether their information is being misused online. The confusion, however, stems from the fact that the terms of the WebWatcher service include a mandatory arbitration and class action waiver provision, which could be interpreted as applying to the claims arising from the breach of Defendants' systems. (*See* Dkt. 1 at ¶ 43; *see also* Starwood Email to Valued Guests and WebWatcher Terms & Conditions, attached as Exhibit B & C, respectively.) Specifically, the terms state that "any controversy or claim arising out of or relating to this Agreement . . . shall be settled by binding arbitration" and that users of the service could not bring claims "as a plaintiff or class member in any purported class or representative proceeding." (*See* Ex. C.)

3. Given the breadth of this language, Plaintiff alleged that Defendants were creating confusion in their communications with class members, as even sophisticated members of the class (i.e., attorneys) could be confused about their legal rights and whether accepting the WebWatcher terms somehow barred individuals from bringing lawsuits. (Dkt. 1 at ¶ 44.)

4. Since the filing of the Complaint in this case, the Parties have conferred several times through counsel and Defendants clarified and confirmed – at the insistence of Plaintiff’s counsel – that Defendants do “not contend the claims of putative class members w[ould] be subject to the terms of service in Kroll’s WebWatcher product.” (Rapp. Decl. at ¶ 4; *see also* December 9, 2018 Email from Gilbert Keteltas, attached as Exhibit D.)

5. As a result, Plaintiff’s counsel files the instant notice to ensure that putative class members have the benefit of understanding Defendants’ stated position, to clear up any confusion that may have resulted from the WebWatcher terms, and to inform the Court that the allegations in the Complaint expressing concern regarding the potential for misleading and/or confusing class members are moot.

Respectfully submitted,

Dated: December 11, 2018

By: /s/ Jeffrey M. Mervis  
One of Plaintiff’s Attorneys

Jeffrey M. Mervis (MD Federal Bar No. 10180)  
jmervis@mervislaw.com  
THE MERVIS LAW FIRM, LLC  
12505 Park Potomac Avenue, 6th Floor  
Potomac, Maryland 20854  
Tel: 301.762.0020

Rafey S. Balabanian\*  
rbalabanian@edelson.com  
Eve-Lynn Rapp\*  
erapp@edelson.com  
EDELSON PC  
123 Townsend Street, Suite 100  
San Francisco, California 94107  
Tel: 415.212.9300  
Fax: 415.373.9435

*\*Pro hac vice* admission to be sought.

**CERTIFICATE OF SERVICE**

I, Jeffrey M. Mervis, an attorney, certify that on December 11, 2018, I caused to be served the above and foregoing ***Notice Regarding Defendants' Intent Not to Enforce WebWatcher Arbitration And Class Action Waiver*** by causing true and accurate copies of such paper to be delivered to Defendants via the Court's CM/ECF system on December 11, 2018.

/s/ Jeffrey M. Mervis

# EXHIBIT A

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

DONNA HITESHEW, individually and on  
behalf of all others similarly situated,

Plaintiff,

v.

MARRIOTT INTERNATIONAL, INC., a  
Delaware corporation, and STARWOOD  
HOTELS & RESORTS WORLDWIDE,  
LLC, a Maryland limited liability company,

Defendants.

Case No.: 8:18-cv-03755

**Honorable Paul W. Grimm**

**DECLARATION OF EVE-LYNN RAPP**

Pursuant to 18 U.S.C. § 1746, I, Eve-Lynn J. Rapp, hereby declare and state as follows:

1. I am an attorney admitted to practice before the Supreme Court of the State of Illinois, and intend to file a motion for leave to appear *pro hac vice* before this Court for purposes of this action. I am entering this Declaration in support of Plaintiff Donna Hiteshew's Notice Regarding Defendants' Intent to Not Enforce WebWatcher Arbitration and Class Action Waiver (the "Notice"). This Declaration is based upon my personal knowledge, except where expressly noted otherwise. If called upon to testify to the matters stated herein, I could and would competently do so.

2. I am a Partner of Edelson PC ("Edelson") which has been retained, along with local counsel, to represent Plaintiff Hiteshew in the above-captioned matter.

3. On December 6, 2018 Plaintiff Hiteshew filed a putative Class Action Complaint against Defendants Marriott International, Inc. and Starwood Hotels & Resorts Worldwide LLC (collectively "Marriott"), arising from the breach of Marriott's security system that exposed the personal data of approximately 500 million people. (Dkt. 1.)

4. Beyond Defendants' lax security, one issue addressed in Plaintiff's Complaint was the confusion being created by Defendants in notifying class members of the breach. Namely, Defendants disseminated emails and directed class members to a website, which among other things, advised of the breach and offered customers one-year of WebWatcher, a web monitoring service that is ostensibly intended to aid people in monitoring whether their information is being misused online. A true and accurate copy of Starwood Email to Valued Guests and WebWatcher Terms & Conditions are attached hereto as Exhibit B and C to Plaintiff's Notice, respectively.

5. Since filing the Complaint in this case, the Parties have conferred several times through counsel. Through the course of those communications, and at the insistence of Plaintiff's counsel, Defendants have clarified and confirmed that they do "not contend the claims of putative class members w[ould] be subject to the terms of service in Kroll's WebWatcher product." A true and accurate copy of Defendants' December 9, 2018 Email is attached Plaintiff's Notice as Exhibit D.

6. Before filing Plaintiff's Notice, Plaintiff's counsel informed Defendants' counsel of the need to alert class members and the Court that Defendants did not intend to enforce the WebWatcher arbitration and class action waiver, and suggested that the Parties do so jointly. However, as of the time of this filing, Defendants' counsel did not respond.

\*

\*

\*

I declare under penalty of perjury that the foregoing is true and correct.

Executed on December 11, 2018 at San Francisco, California.

/s/ Eve-Lynn J. Rapp

# EXHIBIT B



From: Starwood Hotels <[starwoodhotels@email-marriott.com](mailto:starwoodhotels@email-marriott.com)>

Sent: Thursday, December 6, 2018 5:56 PM

Subject: Starwood Guest Reservation Database Security Incident



California Residents | California - Español

العربية | 繁體中文 | 简体中文 | Deutsch

Español (España) | Español (Latinoamérica)

Français (Canadien) | Français | Italiano

日本語 | Português (Europeu) | Português (Brasil)

한국어 | Русский

Dear Valued Guest,

Marriott values our guests and understands the importance of protecting your personal information. We have taken measures to investigate and address a data security incident involving the

Starwood guest reservation database. The investigation has determined that there was unauthorized access to the database, which contained guest information relating to reservations at Starwood properties\* on or before September 10, 2018. This notice explains what happened, measures we have taken, and some steps you can take in response.

## **Starwood Guest Reservation Database Security Incident**

On September 8, 2018, Marriott received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database. Marriott quickly engaged leading security experts to help determine what occurred. Marriott learned during the investigation that there had been unauthorized access to the Starwood network since 2014. Marriott recently discovered that an unauthorized party had copied and encrypted information, and took steps towards removing it. On November 19, 2018, Marriott was able to decrypt the information and determined that the contents were from the Starwood guest reservation database.

Marriott has not finished identifying duplicate information in the database, but believes it contains information on up to approximately 500 million guests who made a reservation at a Starwood property. For approximately 327 million of these guests, the information includes some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences. For some, the information also includes payment card numbers and payment card expiration dates, but the payment card numbers were encrypted using Advanced Encryption Standard encryption (AES-128). There are two components needed to decrypt the payment card numbers, and at this point, Marriott has not been able to rule out the possibility that both were taken. For the remaining guests, the

Case 8:18-cv-03755-PWG Document 6-2 Filed 12/11/18 Page 4 of 18  
information was limited to name and sometimes other data such as mailing address, email address, or other information.

Marriott reported this incident to law enforcement and continues to support their investigation. The company is also notifying regulatory authorities.

Marriott deeply regrets this incident happened. From the start, we moved quickly to contain the incident and conduct a thorough investigation with the assistance of leading security experts. Marriott is working hard to ensure our guests have answers to questions about their personal information with a dedicated website and call center. We are supporting the efforts of law enforcement and working with leading security experts to improve. Marriott is also devoting the resources necessary to phase out Starwood systems and accelerate the ongoing security enhancements to our network.

### **Guest Support**

Marriott has taken the following steps to help you monitor and protect your information:

#### **Dedicated Call Center**

Marriott has established a dedicated call center to answer questions you may have about this incident. The call center is open seven days a week, and is available in multiple languages. Our dedicated call center may experience high volume initially, and we appreciate your patience.

## Email notification

Marriott began sending emails on a rolling basis on November 30, 2018 to affected guests whose email addresses are in the Starwood guest reservation database.

## Free WebWatcher Enrollment

Marriott is providing guests the opportunity to enroll in WebWatcher free of charge for one year. WebWatcher monitors internet sites where personal information is shared and generates an alert to the consumer if evidence of the consumer's personal information is found. Due to regulatory and other reasons, WebWatcher or similar products are not available in all countries. Guests from the United States who complete the WebWatcher enrollment process will also be provided fraud consultation services and reimbursement coverage for free.

The section below provides additional information on steps you can take. If you have questions about this notification and to enroll in WebWatcher (if it is available in your country), please visit [info.starwoodhotels.com](http://info.starwoodhotels.com).

\* Starwood brands include: W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Méridien Hotels & Resorts, Four Points by Sheraton and Design Hotels. Starwood branded timeshare properties are also included.

Best wishes,

A handwritten signature in black ink, appearing to read "Arne Sorenson". The signature is fluid and cursive, with the first name "Arne" and last name "Sorenson" clearly distinguishable.

Arne Sorenson

### **MORE INFORMATION ON STEPS YOU CAN TAKE**

Regardless of where you reside, below are some additional steps you can take.

- Monitor your SPG account for any suspicious activity.
- Change your password regularly. Do not use easily guessed passwords. Do not use the same passwords for multiple accounts.
- Review your payment card account statements for unauthorized activity and immediately report unauthorized activity to the bank that issued your card.
- Be vigilant against third parties attempting to gather information by deception (commonly known as "phishing"), including through links to fake websites. Marriott will not ask you to provide your password by phone or email.

If you believe you are the victim of identity theft or your personal data has been misused, you should immediately contact your national data protection authority or local law enforcement.

**If you are a resident of the United States:**

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

*Equifax*, PO Box 740241, Atlanta, GA 30374,  
[www.equifax.com](http://www.equifax.com), 1-800-685-1111

*Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com),  
1-888-397-3742

*TransUnion*, PO Box 2000, Chester, PA 19016,  
[www.transunion.com](http://www.transunion.com), 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid

identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

*Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)*

**If you are a resident of Connecticut, Maryland, Massachusetts, North Carolina, or Rhode Island**, you may contact and obtain information from your state attorney general at:

*Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, [www.ct.gov/ag](http://www.ct.gov/ag), 1-860-808-5318*

*Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, [www.oag.state.md.us](http://www.oag.state.md.us), 1-888-743-0023 or 1-410-576-6300*

*Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, [www.mass.gov/ago/contact-us.html](http://www.mass.gov/ago/contact-us.html), 1-617-727-8400*



*North Carolina Attorney General's Office*, 9001 Mail Service Center, Raleigh, NC 27699, [www.ncdoj.gov](http://www.ncdoj.gov), 1-919-716-6400 or 1-877-566-7226

*Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, [www.riag.ri.gov](http://www.riag.ri.gov), 1-401-274-4400

**If you are a resident of Massachusetts or Rhode Island**, note that pursuant to Massachusetts or Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze.

**If you are a resident of West Virginia**, you have the right to ask that nationwide consumer reporting agencies place “fraud alerts” in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

**Fraud Alerts:** There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial



Case 8:18-cv-03755-PWG Document 6-2 Filed 12/11/18 Page 10 of 18

fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

**Credit Freezes:** You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

**Experian Security Freeze**, PO Box 9554, Allen, TX 75013,  
[www.experian.com](http://www.experian.com)

**TransUnion Security Freeze**, PO Box 2000, Chester, PA  
19016, [www.transunion.com](http://www.transunion.com)

**Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348,  
[www.equifax.com](http://www.equifax.com)

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password

Case 8:18-cv-03755-PWG Document 6-2 Filed 12/11/18 Page 12 of 18  
or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

**Fair Credit Reporting Act:** You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (<https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>), and that article refers individuals seeking more information to visit [www.ftc.gov/credit](http://www.ftc.gov/credit). The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.
- Each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion – is required to provide you with a free copy of your credit report, at your request, once every 12 months.
- You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited. You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you receive based on information in your credit report.
-

- Identity theft victims and active duty military personnel have additional rights.

**If You Are A European Union Data Subject**, you may contact or obtain information from your Data Protection Authority at:

*Austria*: Österreichische Datenschutzbehörde,  
[Wickenburggasse 8](#), 1080 Vienna, +43 1 52 152 0, Email:  
[dsb@dsb.gv.at](mailto:dsb@dsb.gv.at)

*Belgium*: De Gegevensbeschermingsautoriteit (GBA), [Rue de la Presse 35](#), 1000 Brussels, +32 (0)2 274 48 00, Email:  
[contact@apd-gba.be](mailto:contact@apd-gba.be)

*Bulgaria*: Commission for Personal Data Protection (CPDP), [2 Prof. Tsvetan Lazarov Blvd.](#), [Sofia](#) 1592, +359 899 877 156,  
Email: [kzld@cpdp.bg](mailto:kzld@cpdp.bg)

*Croatia*: Croatian Personal Data Protection Agency (AZOP),  
[Fra Grge Martića 14](#), HR-10 000 Zagreb, +385 (0)1 4609-000,  
Email: [azop@azop.hr](mailto:azop@azop.hr)

Protection, [Iasonos 1](#), 1082 Nicosia (office address), P.O. Box 23378, 1682 Nicosia, Cyprus (postal address), +357 22818456, Email: [commissioner@dataprotection.gov.cy](mailto:commissioner@dataprotection.gov.cy)

*Czechia (Czech Republic):* The Office for Personal Data Protection, [Pplk. Sochora 27](#), 170 00 Praha 7, +420 234 665 111, Email: [posta@uouu.cz](mailto:posta@uouu.cz)

*Denmark:* Datatilsynet, [Borgergade 28, 5](#), 1300 København, +45 33 19 32 00 (Monday – Thursday 9:00am to 12:00pm and 12:30 to 3:30pm, Friday 9:30am to 12:00pm), Email: [dt@datatilsynet.dk](mailto:dt@datatilsynet.dk)

*Estonia:* Andmekaitse Inspektsioon, [19 Väike-Ameerika St.](#), 10129 Tallinn, +372 627 4135, Email: [info@aki.ee](mailto:info@aki.ee)

*Finland:* Tietosuojavaltuutetun toimisto, [Ratapihantie 9, 6th Floor, 00520, Helsinki](#) (office address), P.O. Box 800, 00521 Helsinki (postal address), +358 29 566 6700, Email (registry): [tietosuoja@om.fi](mailto:tietosuoja@om.fi)

*France:* Commission nationale de l'informatique et des libertés (CNIL), [3 Place de Fontenoy](#) TSA 80715, 75334 PARIS CEDEX 07, +33 01 53 73 22 22 (Monday to Thursday 9:00am to 6:30pm, Friday 9:00am to 6:00pm)

*Germany:* Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), [Husarenstr. 30 - 53117 Bonn](#), +49 (0)228-997799-0, Email: [poststelle@bfdi.bund.de](mailto:poststelle@bfdi.bund.de). (You may also contact the Data Protection Agency in your Bundesland.)

*Greece:* Data Protection Authority Offices, Kifissias 1-3, 115 23 Athens, +30-210 6475600, Email: [contact@dpa.gr](mailto:contact@dpa.gr)

*Hungary:* Nemzeti Adatvédelmi és Információszabadság Hatóság, H-1125 [Budapest, Szilágyi Erzsébet fasor 22/C](#), +36 1 391 1400, Email: [privacy@naih.hu](mailto:privacy@naih.hu)

*Ireland:* Data Protection Commission (Comisiún Cosanta Sonraí), Canal House, Station Road, Portarlinton, R32 AP23 Co. Laois, +353 57 868 4800, +353 (0761) 104 800, Email: [info@dataprotection.ie](mailto:info@dataprotection.ie)

*Italy:* Garante per la protezione dei dati personali, Piazza Venezia 11 – 00187 Roma, +39 06 6967 71, +39 06 6967 72917, Email: [urp@gpdp.it](mailto:urp@gpdp.it)

*Latvia:* Data State Inspectorate, [Blaumana Street 11 / 13–11](#), Riga, LV–1011, +371 67 22 31 31 (1:00 to 3:00pm), Email: [info@dvi.gov.lv](mailto:info@dvi.gov.lv)



*Juozapavičiaus g. 6, 09310 Vilnius* 6, 09310 Vilnius, +370 (8 5) 271 2804, 279 1445, Email: paštas [ada@ada.lt](mailto:ada@ada.lt)

*Luxembourg*: Commission Nationale Pour La Protection Des Données (CPND), [1, avenue du Rock'n'Roll, L-4361 Esch-sur-Alzette](#), +352 26 10 60 – 1

*Malta*: Office of the Information and Data Protection  
Commissioner (IDPC), Level 2, Airways House, High Street,  
Sliema SLM 1549, +356 2328 7100, Email:  
[idpc.info@idpc.org.mt](mailto:idpc.info@idpc.org.mt)

*Netherlands*: Autoriteit Persoonsgegevens, Postbus 93374,  
2509 AJ DEN HAAG, +31 (0)70 888 85 00

*Poland*: Urząd Ochrony Danych Osobowych, ul. [Stawki 2, 00-193 Warszawa](#), +48 22 531 03 00, Email:  
[kancelaria@uodo.gov.pl](mailto:kancelaria@uodo.gov.pl)

*Portugal*: Comissão Nacional de Protecção de Dados (CNPd),  
[Av. D. Carlos I, 134 - 1.º, 1200-651 Lisboa](#), +351 21 392 84 00,  
Email: [geral@cnpd.pt](mailto:geral@cnpd.pt)

*Romania*: Autoritatea Națională de Supraveghere a Prelucrării  
Datelor cu Caracter Personal (ANSPDCP), [28-30 G-ral](#)



Case 8:18-cv-03755-PWG Document 6-2 Filed 12/11/18 Page 18 of 18  
[REDACTED]  
[Gheorghe Magheru](#) Bld., District 1, post code 010336,  
Bucharest, +40 318 059 211, Email: [presa@dataprotection.ro](mailto:presa@dataprotection.ro),  
[anspdcpc@dataprotection.ro](mailto:anspdcpc@dataprotection.ro)

*Slovakia*: Úrad na ochranu osobných údajov, [Hraničná 12](#), 820  
07, Bratislava 27, +421 2 32313214, Email:  
[statny.dozor@pdp.gov.sk](mailto:statny.dozor@pdp.gov.sk)

*Slovenia*: Informacijski pooblaščenec, [Dunajska cesta 22](#), SI-  
1000 Ljubljana, +386 1 230 97 30, Email: [gp.ip@ip-rs.si](mailto:gp.ip@ip-rs.si)

*Spain*: Agencia Española de Protección de Datos (AEPD),  
[Jorge Juan, 6](#), 28001 Madrid, +34 913 996 207, Email:  
[contratacion@agpd.es](mailto:contratacion@agpd.es)

*Sweden*: Datainspektionen, Box 8114, 104 20 Stockholm, +46  
08 657 61 00 (Monday, Tuesday, Thursday, Friday: 9:00 to  
11:00am; Wednesday: 9:30 to 11:30am), Email:  
[datainspektionen@datainspektionen.se](mailto:datainspektionen@datainspektionen.se)

*United Kingdom*: Information Commissioner's Office (ICO),  
Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF,  
+44 0303 123 1113, +44 01625 545 745, Email:  
[dataprotectionfee@ico.org.uk](mailto:dataprotectionfee@ico.org.uk)

# EXHIBIT C

# Terms & Conditions

## Terms & Conditions for the United States & Canada

### Terms & Conditions: United States

If you are located in the United States or its territories, the following terms and conditions will apply:

#### 1. Your Use of the Web Portal, Services, and Products

By enrolling, accessing, and/or using the products and/or services ("Services") offered by Kroll Information Assurance, LLC. ("Kroll," "we," "you," "our," or "us") and this web portal (the "Portal"). The Portal is also referred to herein as the "Platform." you represent that you are over eighteen (18) years of age, and acknowledge that you have read, understood, and agreed to the terms herein ("Agreement"), and will follow all applicable laws and regulations.

#### 2. Privacy and Information Sharing

Please review our Privacy Policy (<https://enroll.idmonitoringservice.com/privacy-policy>), (available on this Platform), which is incorporated into this Agreement, to ensure that you understand how we collect, use and disclose information about you. Our use of your personal information is subject to the terms of our Privacy Policy (<https://enroll.idmonitoringservice.com/privacy-policy>), and you consent to our use in accordance with those terms.

#### 3. Cancellation

Upon cancellation, your account will be deactivated, and you will no longer be able to log into our Portal and/or have access to the Services.

#### 4. Disclaimer of Warranties

A. Some jurisdictions either do not allow or place restrictions in certain types of agreements upon the exclusion or limitation of warranties, conditions, liability for loss or damage. Only the limitations and exclusions which are lawful in your jurisdiction will apply to you and our liability will be limited to the maximum extent permitted by law.

B. Our Portal, including all content, memberships, products and services made available on or accessed through this Portal (collectively, "Portal Services"), is provided to you "AS IS". To the extent permissible under applicable law, Kroll and its officers, directors, employees, and agents, subsidiaries, affiliates, contractors, third party data sources and suppliers ("Representatives") disclaim all express and implied warranties, including those of title, merchantability, and fitness for a particular purpose, non-infringement, and informational content.

C. you agree that you will access and use our Portal and Portal Services solely at your own risk.

#### 5. Indemnification

A. You agree to indemnify, defend, and hold harmless Kroll and its representatives (collectively, the "Indemnified Party") from and against all third party claims, losses, expenses, damages and costs, including reasonable attorney's fees, arising out of, in connection with, or resulting from (i) your use of the Portal, the Portal Services, or the Services; (ii) from any violation of the terms of this Agreement by you or caused by you; or (iii) your violation of applicable laws, rules or regulations.

B. If the Indemnified Party is subject to any claim for which the Indemnified Party may be indemnified by you, the Indemnified Party may, at your expense, assume the exclusive defense and control of any such claim, and you will not settle any claim without the Indemnified Party's prior written consent.

#### 6. Limitation of Liability

A. except as otherwise specified, you expressly understand and agree that Kroll and its Representatives shall not be liable to you for:

any incidental, special, consequential, or exemplary damages which may be incurred by you, however caused and under any theory of liability. This shall include, but not be limited to any loss of profit (directly or indirectly), any loss of goodwill, any loss of data suffered, cost of procurement or substitute goods or services, or other intangible loss.

B. The limitations of our liability to you shall apply whether or not we have been advised or should have been aware of the possibility of any such losses arising.

C. you agree that, to the extent permitted by law, Kroll's total liability to you (and any of your minor children) for any or all of your losses or injuries (or those of your minor children) from Kroll's or its agents' or its representatives' acts or omissions, regardless of the nature of the legal or equitable claim, shall not exceed \$1,000 (one thousand dollars) in the aggregate.

#### 7. "Written Instructions" and Provision of Personal Information

##### A. "Written Instructions"

You understand that by accepting these Terms and Conditions you are providing "written instructions" to CSIDentity Corporation ("CSID") and its employees, agents, subsidiaries, affiliates, contractors, third party data and service providers, and, **only where applicable to the Services provided**, to all other credit reporting agencies under the Fair Credit Reporting Act ("FCRA"), as amended, including Experian, TransUnion, Equifax and affiliated entities, to access your credit files from each national credit reporting agency and to exchange information about you with each national credit reporting agency in order to verify your identity and to provide the services to you. Where applicable to the Services, you agree and hereby authorize CSID to provide your personally identifiable information (or, if applicable, information about any minor children you have enrolled) to third parties as provided in CSID's Privacy Policy (<https://www.csid.com/privacy-policy/>), as may be amended from time to time, in order to provide the services to you (and to those children you have enrolled). You further authorize CSID to obtain information and reports about you (or about any children you have enrolled, if applicable) in order to provide the services, including, but not limited to, credit monitoring services, credit reporting, identity monitoring, fraud resolution services, restoration services, address history reports, name and alias reports, criminal reports or sex offender reports, and to provide monitoring and alerts. You may review the CSID Privacy Policy here (<https://www.csid.com/privacy-policy/>).

##### B. Provision of Personal Information

While enrolling for the Services, we may ask you for the following types of information: name, address, phone number, and e-mail address; date of birth, driver's license number and social security number; and other personal information to verify your identity and financial information (such as credit card number). This information may be required in order to verify your identity and fulfill our obligation to provide our Services to you, including communicating with third parties as necessary to provide such Services (such as identification verification companies, consumer reporting agencies, payment validation companies, law enforcement agencies, or others). By enrolling in identity monitoring Services, including dark web monitoring, you consent to and authorize us to provide your personal information to CSID and for CSID and its agents and employees to obtain and monitor your personal information and provide you alerts as part of the identity monitoring Services. You also consent to the collection by CSID of your personal information from the dark web (both before and after the acceptance of these terms) for the limited purpose of monitoring your personal information through the identity monitoring services, including dark web monitoring.

#### 8. Fair Credit Reporting Act ("FCRA")

FCRA allows you to obtain from each credit reporting agency a disclosure of all the information in your credit file at the time of the request. Full disclosure of information in your file at a credit reporting agency must be provided to you by the credit reporting agency. The information provided to you by the credit reporting agency is intended to constitute the disclosure of information by a credit reporting agency as required by FCRA or similar laws.

Under FCRA, you are entitled to obtain an annual free disclosure of your credit report from each of the national credit reporting agencies. To request your free annual report under FCRA, you must complete an online form, available at <http://www.annualcreditreport.com>. (http://www.annualcreditreport.com/) You may also call a toll-free number at (877) 322-8228, or submit an annual credit report request form via mail (the form is available at <http://www.annualcreditreport.com>).

You are entitled to receive a free copy of your credit report from a credit reporting agency if:

- you have been denied or were otherwise notified of an adverse action related to credit, insurance, employment, or a government granted license or other government granted benefit within the past sixty (60) days, based on information in a credit report provided by such agency.
- you have been denied house/apartment rental or were required to pay a higher deposit than usually required within the past sixty (60) days, based on information in a credit report provided by such agency.
- you certify in writing that you are unemployed and intend to apply for employment during the sixty (60) day period beginning on the date on which you made such certification.
- you certify in writing that you are a recipient of public welfare assistance.
- you certify in writing that you have reason to believe that your file at such credit reporting agency contains inaccurate information due to fraud.

In addition, if you reside in the state of Colorado, Maine, Maryland, Massachusetts, New Jersey, or Vermont, you are entitled to receive a free copy of your credit report once a year and if you reside in the state of Georgia, you are entitled to receive a free copy of your credit report twice a year. Otherwise, a consumer reporting agency may impose a reasonable charge for providing you with a copy of your credit report.

FCRA provides that you may dispute inaccurate or incomplete information in your credit report. You are not required to purchase your credit report from any of the credit bureaus in order to dispute inaccurate or incomplete information in your report or to receive a copy of your report from Equifax, Experian or TransUnion (the three (3) national credit reporting agencies), or from any other credit reporting agency, based on the above-described circumstances.

It may be the policies of Equifax, Experian and/or TransUnion to provide a complimentary copy of the consumer credit report under circumstances other than those described above. If you wish to contact Equifax, Experian or TransUnion to obtain a copy of your credit report directly from such agency or if you wish to dispute information contained in an Equifax, Experian or TransUnion credit report file, please contact those entities directly.

#### 9. Applicable Law and Jurisdiction; Jury Waiver; Class Action Waiver

A. This Agreement shall be governed, interpreted, and enforced according to the laws of the State of Tennessee, regardless of Tennessee conflict of laws.

B. You irrevocably and unconditionally consent and submit to the exclusive jurisdiction of the federal and state courts located in Davidson County, Tennessee for any dispute or litigation arising out of, relating to, or the receipt, use, or purchase of Services from Kroll or its Representatives via this Platform.

#### C. Arbitration; Jury Waiver.

Any controversy or claim arising out of or relating to this Agreement, or the breach hereof, shall be settled by binding arbitration administered in Nashville, Tennessee by the American Arbitration Association ("AAA") in accordance with its Arbitration Rules then in effect. There shall be one arbitrator agreed to by you and Kroll (or its Representatives, as applicable) within twenty (20) days of a written request for arbitration. If the parties cannot agree, an arbitrator will be appointed by the AAA in accordance with its Arbitration Rules. Any award from any such arbitration proceeding may be entered as a judgment in any court of competent jurisdiction. Each party shall bear its own costs in connection with any arbitration hereunder. Nothing herein shall prevent a party from seeking injunctive relief (or any other provisional remedy) from any court having jurisdiction over the parties and the subject matter of the dispute as is necessary to protect such party's proprietary rights.

You and Kroll agree that, to the fullest extent permitted by law, you and Kroll knowingly, voluntarily, and intentionally waive the right to a trial by jury in any action or other legal proceeding arising out of or relating to the Agreement, the Platform or the Services. The foregoing waiver applies to any action or legal proceeding, whether sounding in contract, tort or otherwise. You also agree not to include any employee of Kroll as a party in any such action or proceeding.

D. Class Action Waiver. You and Kroll (or its Representatives, as applicable) knowingly, voluntarily, and intentionally agree that each may bring claims against the other or a Representative only in your or its individual capacity, and not as a plaintiff or class member in any purported class or representative proceeding.

#### 10. Your Passwords and Account Security; Online Access

A. Password and Account Security: Failure to comply with the below requirements shall constitute a breach of these terms and conditions and shall constitute grounds for immediate termination of your account and your right to use the Platform.

You understand that you are responsible for, and agree to:

- i. be solely responsible to Kroll for all activities that occur under your account; and
- ii. notify Kroll immediately if you become aware of any unauthorized use or disclosure, loss, or theft of your password or of your account.

#### B. Online access

- i. If you choose to sign up for the Services online, then you agree that you will not receive any communications or Services via postal mail.
- ii. Online access to consumer credit report information is subject to verification of the identity of the user.

#### 11. Termination of Relationship

A. Termination by You. If you want to terminate your legal agreement with us, you may do so, for any reason, at any time, by cancelling your Service(s) and/or closing your account(s).

#### B. Termination by Kroll.

##### 1. For Cause:

a. We may terminate the Agreement if you have breached the Agreement or if you commit (or cause to be committed) negligence, fraud, willful misconduct or unlawful conduct arising from, in connection with or related to use of Kroll's Services or Platform.

b. If Kroll terminates the Agreement with you for cause, you will forfeit the remainder of your Services.

C. **Effect of Termination.** Provisions of the Agreement which by their nature are intended to survive termination of the Agreement shall survive termination of the Agreement.

## 12. Miscellaneous

A. No waiver of any breach of any provision of this Agreement or of any agreement with us will constitute a waiver of any prior, concurrent, or subsequent breach of the same or other provisions. All waivers must be in writing. If any court of competent jurisdiction finds any part or provision of this Agreement or of any other agreement between you and us to be invalid or unenforceable, such findings will have no effect on any other part or provision of this Agreement or any other agreement between you and us.

B. We are not responsible for delay or failure to perform due to causes beyond our reasonable control.

C. This Agreement constitutes the whole legal agreement between you and us and govern your use of the Services (but excluding any services which we may provide to you under a separate written agreement), and completely replaces any prior agreements between you and us in relation to the Services. Kroll may update this Agreement or any related policy (such as the [Privacy Policy \(https://enroll.idmonitoringservice.com/privacy-policy\)](https://enroll.idmonitoringservice.com/privacy-policy)) from time to time by posting revisions on the Platform.

D. Except as otherwise provided, we may send any notices to you to the most recent e-mail address you have provided to us or, if you have not provided an e-mail address, to any e-mail or postal address that we reasonably believe is your address. If you wish to update your registration information, please log in to your account and update your information.

E. When you provide us with comments, suggestions, or ideas (collectively, "**Feedback**"), such Feedback is not considered confidential and becomes the property of Kroll. We are not obligated to you for any reason if you provide such Feedback. We are free to use, copy, or distribute the Feedback to others for any purpose.

F. We are not a credit repair organization or similarly regulated organization under other applicable laws, and do not provide credit repair advice.

G. Our credit monitoring offerings monitor only the credit file associated with the purchasing consumer, and do not monitor, compare or cross-reference the credit file associated with the purchasing consumer to any other credit file(s) maintained by the applicable credit bureau(s).

Effective Date: November 30, 2018

## **Terms & Conditions: Canada**

**If you are located in Canada, the following Terms & Conditions will apply:**

### 1. Your Use of the Web Portal, Services, and Products

By enrolling, accessing, and/or using the products and/or services ("**Services**") offered by Kroll Information Assurance, LLC ("**Kroll**", "**we**", "**our**", or "**us**") and this web portal (the "**Portal**"), you ("**you**") agree to be bound by these Terms and Conditions (the "**Agreement**"). The Portal is also referred to herein as the "**Platform**". You represent and warrant that you have reached the age of majority in the jurisdiction in which you reside, and you confirm that you have read, understood, and agree to the terms and conditions of this Agreement, and agree to comply with all applicable laws, rules and regulations ("**Applicable Laws**").

### 2. Privacy and Information Sharing

Please review our [Privacy Policy \(https://enroll.idmonitoringservice.com/privacy-policy\)](https://enroll.idmonitoringservice.com/privacy-policy) (available on this Portal), which is incorporated into this Agreement, to understand how we collect, use and disclose information about you.

### 3. Disclaimer of Warranties

A. Some jurisdictions, including Quebec, either do not allow or place restrictions in certain types of agreements upon the exclusion or limitation of warranties, conditions, liability for loss or damage. Only the limitations and exclusions which are lawful in your jurisdiction will apply to you and our liability will be limited to the maximum extent permitted by law. You may have additional rights under applicable laws.

B. Our Platform, including all content, memberships, products and services made available on or accessed through this Platform (collectively, "**Platform Services**"), is provided to you "AS IS". To the extent permissible under applicable law, Kroll and its officers, directors, employees, mandataries, agents, subsidiaries, affiliates, contractors, third party data sources and suppliers ("**Representatives**") disclaim all legal, express and implied warranties and conditions, including those of title, merchantability, quality and fitness for a particular purpose, title and non-infringement of third-party rights and/or third-party content.

C. You agree that you will access and use our Platform, Platform Services, and Services solely at your own risk.

### 4. Indemnification

A. You agree to indemnify, defend, and hold harmless Kroll and its Representatives (collectively, the "**Indemnified Party**") from and against all third party claims, losses, expenses, damages and costs, including reasonable legal fees, arising out of, in connection with, or resulting from (i) your use of the Platform, Platform Services, or the Services; (ii) from any violation of the terms or conditions of this Agreement by you or caused by you; or (iii) your violation of Applicable Laws.

B. If the Indemnified Party is subject to any claim for which the Indemnified Party may be indemnified by you, the Indemnified Party may, at your expense, assume the exclusive defense and control of any such claim, and you will not settle any claim without the Indemnified Party's prior written consent.

### 5. Limitation of Liability

THE LAWS OF CERTAIN JURISDICTIONS, INCLUDING QUEBEC, DO NOT ALLOW THE EXCLUSION OR LIMITATION OF CERTAIN LIABILITIES. IF THESE LAWS APPLY TO YOU, SOME OR ALL OF THE EXCLUSIONS OR LIMITATIONS BELOW MAY NOT APPLY TO YOU, AND YOU MAY HAVE ADDITIONAL RIGHTS.

A. Except as otherwise specified, you expressly understand and agree that Kroll and its representatives shall not be liable to you for any incidental, special, consequential, punitive or exemplary damages which may be incurred by you, however caused and under any theory of liability, whether in contract, tort (including negligence), civil liability or otherwise. This shall include, but not be limited to (directly or indirectly) any loss of profit, any loss of goodwill, any loss of data suffered, cost of procurement or substitute goods or services, or other intangible loss. These exclusions of our liability shall apply to you whether or not we have been advised or should have been aware of the possibility of any such damages arising.

B. You agree that, to the extent permitted by Applicable Laws, Kroll's total liability to you (and any of your minor children) for any or all of your losses or injuries (or those of your minor children) from Kroll's, or its mandataries', agents' or representatives' acts or omissions, regardless of the nature of the legal or equitable claim, shall not exceed \$1,000 (one thousand dollars) in the aggregate. The foregoing liability shall apply in respect of any theory of liability, whether in contract, tort (including negligence), civil liability or otherwise, and whether or not we have been advised or should have been aware of the possibility of any such damages arising.

### 6. Third Party Terms

Case 8:18-cv-03755-PWG Document 6-3 Filed 02/11/18 Page 5 of 6

Certain of our identity monitoring services are provided through our third-party data and service provider, CSIDentity Corporation ("CSID"). By enrolling in identity monitoring services, including dark web monitoring, you consent to the use of your information by CSID to obtain and monitor your personal information and provide you alerts as part of the identity monitoring services. You also consent to the collection by CSID of your personal information from the dark web (both before and after the acceptance of these Third Party Terms) for the limited purpose of monitoring your personal information through the identity monitoring services, including dark web monitoring, and agree that such collection by CSID is clearly in your interest. You may review the CSID Privacy Policy [here](https://www.csid.com/privacy-policy/) (<https://www.csid.com/privacy-policy/>).

7. Applicable Law and Jurisdiction; Arbitration; Jury Waiver; Class Action Waiver

A. This Agreement shall be governed, interpreted, and enforced according to the laws of the State of Tennessee, regardless of Tennessee conflict of laws, unless the laws of the jurisdiction where you reside require that the laws of such jurisdiction to apply. The terms of this section 7 shall apply only to the extent permitted by your jurisdiction, including Quebec.

B. Any controversy or claim arising out of or relating to this Agreement, or the breach thereof, shall be settled by binding arbitration administered in Nashville, Tennessee by the American Arbitration Association ("AAA") in accordance with its Arbitration Rules then in effect. There shall be one arbitrator agreed to by you and Kroll (or its Representatives, as applicable) within twenty (20) days of a written request for arbitration. If the parties cannot agree, an arbitrator will be appointed by the AAA in accordance with its Arbitration Rules. Any award from any such arbitration proceeding may be entered as a judgment in any court of competent jurisdiction. Each party shall bear its own costs in connection with any arbitration hereunder. Nothing herein shall prevent a party from seeking injunctive relief (or any other provisional remedy) from any court having jurisdiction over the parties and the subject matter of the dispute as is necessary to protect such party's proprietary rights.

B. For any dispute resolution not subject to the arbitration provision above, you irrevocably and unconditionally consent and submit to the exclusive jurisdiction of the federal and state courts located in Davidson County, Tennessee for any dispute or litigation arising out of, relating to, or the use or purchase of Services from Kroll via this Platform or any matter relating to this Agreement unless the laws of the jurisdiction where you reside require that a venue located in such jurisdiction to hear such matters.

C. Jury Waiver

You and Kroll agree that, to the fullest extent permitted by law, you and Kroll knowingly, voluntarily, and intentionally wave the right to a trial by jury in any action or other legal proceeding arising out of or relating to the Agreement, the Platform or the Services. The foregoing waiver applies to any action or legal proceeding, whether sounding in contract, tort or otherwise. You also agree not to include any employee of Kroll as a party in any such action or proceeding.

D. Class Action Waiver

Some jurisdictions, including Quebec, do not allow a waiver of the right to file a class action in certain circumstances so that the following waiver may not apply to you. To the maximum extent permitted by Applicable Laws, you and Kroll (or its Representatives, as applicable) knowingly, voluntarily, and intentionally agree that each may bring claims against the other, or any Representative, only in your or its individual capacity, and not as a plaintiff or class member in any purported class or representative proceeding.

8. Your Passwords and Account Security; Online Access

A. Password and Account Security

Failure to comply with the below requirements shall constitute a breach of the Agreement and shall constitute grounds for immediate termination of your account and your right to use the Platform.

You understand that you are responsible for, and agree to:

- i. be solely responsible to Kroll for all activities that occur under your account; and
- ii. notify Kroll immediately if you become aware of any unauthorized use or disclosure, loss, or theft of your password or of your account.

B. Online access

- i. If you choose to sign up for the Services online, then you agree that you will not receive any communications or Services via postal mail.
- ii. notify Kroll immediately if you become aware of any unauthorized use or disclosure, loss, or theft of your password or of your account.

9. Termination of Relationship

A. Termination by You If you want to terminate the Agreement, you may do so, for any reason, at any time, by cancelling your subscription(s) and/or closing your account(s).

B. Termination by Kroll

1. For Cause

a. We may terminate the Agreement if you have breached the Agreement or if you commit (or cause to be committed) negligence, fraud, willful misconduct or unlawful conduct arising from, in connection with or related to use of Kroll's Services or Platform.

b. If Kroll terminates the Agreement with you for cause, your subscription will terminate immediately.

2. For Convenience

We may terminate the Agreement for convenience. In such case, Kroll will provide thirty (30) days' prior written notice of such termination, where practicable.

C. Effect of Termination

Provisions of the Agreement which by their nature are intended to survive termination of the Agreement shall survive termination of the Agreement.

10. Miscellaneous

A. No waiver of any breach of any provision of this Agreement or of any agreement with us will constitute a waiver of any prior, concurrent, or subsequent breach of the same or other provisions. All waivers must be in writing. If any court of competent jurisdiction finds any part or provision of this Agreement or of any other agreement between you and us to be invalid or unenforceable, such findings will have no effect on any other part or provision of this Agreement or any other agreement between you and us.

B. We are not responsible for delay or failure to perform due to causes beyond our reasonable control.

C. This Agreement constitutes the whole legal agreement between you and us and govern your use of the Services, Portal, and the Platform (but excluding any services which we may provide to you under a separate written agreement), and completely replaces any prior agreements between you and us in relation to same. Kroll may update this Agreement or any related policy (such as the [Privacy Policy](https://enroll.idmonitoringservice.com/privacy-policy/), (<https://enroll.idmonitoringservice.com/privacy-policy/>)) from time to time by posting revisions on the Platform.

D. Except as otherwise provided, we may send any notices to you to the most recent e-mail address you have provided to us or, if you have not provided an e-mail address, to any e-mail or postal address that we reasonably believe is your best contact information. We may update our information for e-mail or postal address for our account to reflect your information.

E. When you provide us with comments, suggestions, or ideas (collectively, "Feedback"), such Feedback is not considered confidential and becomes the property of Kroll. We are not obligated to you for any reason if you provide such Feedback. We are free to use, copy, or distribute the Feedback to others for any purpose.

F. We are not a credit repair organization or similarly regulated organization under other Applicable Laws, and do not provide credit repair advice.

G. You agree that you will use the Services to protect against or prevent actual fraud, unauthorized transactions, claims or other liabilities.

H. It is the express wish of the parties that this Agreement and all related documents be drawn up in English. C'est la volonté expresse des parties que la présente convention ainsi que tous les documents qui s'y rattachent soient rédigés en anglais.

Effective Date: November 30, 2018

This website makes use of technical cookies and cookies set by third parties. If you need further information about cookies or would like to disable a specific cookie (or all of them), please click [here \(https://enroll.idmonitoringservice.com/privacy-policy\)](https://enroll.idmonitoringservice.com/privacy-policy). By continuing to browse by accessing any other section of this website or selecting any item on it (e.g. by clicking a picture or a link), this will imply your consent to this website's use of cookies.

# EXHIBIT D





---

## Fwd: Hiteshew v Marriott International, Inc.

---

----- Forwarded message -----

From: **Keteltas, Gilbert S.** <[gketeltas@bakerlaw.com](mailto:gketeltas@bakerlaw.com)>

Date: Sun, Dec 9, 2018 at 12:58 PM

Subject: RE: Hiteshew v Marriott International, Inc.

To: Eve-Lynn Rapp <[erapp@edelson.com](mailto:erapp@edelson.com)>

Cc: Warren, Daniel <[DWarren@bakerlaw.com](mailto:DWarren@bakerlaw.com)>, Rafey Balabanian <[rbalabanian@edelson.com](mailto:rbalabanian@edelson.com)>, [Dave.Bell@marriott.com](mailto:Dave.Bell@marriott.com) <[Dave.Bell@marriott.com](mailto:Dave.Bell@marriott.com)>, Ghannoum, Lisa M. <[lghannoum@bakerlaw.com](mailto:lghannoum@bakerlaw.com)>, Jay Edelson <[jedelson@edelson.com](mailto:jedelson@edelson.com)>, Shawn Davis <[sdavis@edelson.com](mailto:sdavis@edelson.com)>, [cdore@edelson.com](mailto:cdore@edelson.com) <[cdore@edelson.com](mailto:cdore@edelson.com)>

Eve-

As to WebWatcher, Marriott does not contend the claims of putative class members will be subject to the terms of service in Kroll's WebWatcher product.

On the technical issues you shared with us a few hours ago, we feel confident that there is no need to involve the court on a motion for emergency relief and will be back to you, hopefully within a few hours, with further confirmation.

In short, we do not believe the signatory to a motion for a temporary restraining order could fairly certify that the filing was based on a reasonable inquiry. And the suggestion that you may file and withdraw the motion anyway – as you have done before – should be a factor the court considers when it makes determinations concerning leadership in what will likely be a future MDL.

**Gil Keteltas**  
Partner

---

**BakerHostetler**

Washington Square  
1050 Connecticut Ave, N.W. | Suite 1100  
Washington, DC 20036-5403  
T +1.202.861.1530

[gketeltas@bakerlaw.com](mailto:gketeltas@bakerlaw.com)  
[bakerlaw.com](http://bakerlaw.com)

