

Terms of Use

Version 2.3—Effective on: 12 June, 2023.

These Terms of Use (the “**TOU**”) are between you, the user of the Flare Platform (as defined below), and Flare Systems, Inc., with a registered address at 1751 Rue Richardson, Montréal, Québec, H3K 1G6, Canada (“**Flare**”).

The TOU enters into force upon your acceptance, such as if you create an account or access your account for the first time on the Flare Platform, or otherwise, whenever you access and use our Services (as defined below) and continue in full force for as long as you are using our Services, unless the TOU is terminated as set forth herein. If you have any questions on the TOU, you can reach out to us by e-mail at legal@flare.io.

1. DEFINITIONS

- “**Customer**” means an entity with whom we have an agreement to provide you with the Services.
- “**Confidential Information**” means any information, including, without limitation, all computer programs, codes, algorithms, know-how, processes, formulas, marketing plans, strategic plans, and other technical, business, financial and product development data, that should reasonably be known as confidential.
- “**Content**” refers to any data, material, content, or software made available to you through the Flare Platform, or obtained through the Flare Platform, including Public Data, search results, intelligence data, contextual explanations, alerts resulting from the Monitoring Services, or any content retrieved using the Retrieval Function. The Content also includes risk scores and contextual information on the search results generated by our algorithms.
- “**Documentation**” means the documentation available at the following URL, as modified from time to time: <https://docs.flare.io/>.
- “**Flare Platform**” means the web application, mobile application, search bar, search API, application programming interface, software and other components described in the Documentation, and made available to you by Customer.
- “**Intended Purposes**” means to prevent fraud, defamation, abuse of rights, crimes, and incidents, including for threat intelligence purposes, such as to monitor the dark web for leaked data.
- “**IP**” means all intellectual property, including, without limitation, works, inventions (whether patentable or not), discoveries, improvements, trade secrets, know-how, scientific formulas, data, information, images, reports, results, analysis, software, models, research and development information, technical information, prototypes, specifications, patterns, drawings, algorithms, products, compositions, processes and protocols, methods, tests, devices, computer programs, trade-marks and any and all proprietary rights provided under patent law, copyright law, trade-mark law, design patents or industrial design law, semiconductor chip or mask work law, or any other statutory provision or civil or common law principle applicable to the protection of intangible proprietary information or rights, including trade secret law, which may provide a right in any of the foregoing as well as any and all applications, registrations or other evidence of a right in any of the foregoing.
- “**Losses**” means any claims, damages, fines, costs, and expenses, including reasonable attorney’s fees, where applicable.
- “**Monitoring Services**” means the use of the Flare Platform to monitor dark web forums, open ports, S3 buckets, ransomware blogs, public GitHub repositories, paste sites, dark

- web marketplaces, dark web chats, threat actors' profiles, infected device market, illicit telegram markets and similar data sources as determined by Flare from time to time (the **"Monitored Sources"**).
- **"Public Data"** means all data and content made available to you through Monitored Sources, including those retrieved through the Retrieval Function, or any other publicly available content available through the Flare Platform.
 - **"Representatives"** means Flare, our affiliates, licensors, suppliers, employees, directors, contractors, and officers.
 - **"Retrieval Function"** means a functionality of the Flare Platform that allows for the retrieval of data, software, content, or material from the Monitored Sources. A retrieval includes the extraction, download, control, and possession.
 - **"Services"** means the services provided to Customer by Flare, and which Customer allows you to access through an authorized account including as applicable, access and use of Flare Platform, along with any applications, application programming interfaces (**"API"**), technologies, software, technical support services, Documentation, and content made available to you by Flare, and which Customer allows you to access through an authorized account.

2. YOUR ACCOUNT

You must have an account to use the Services. You are responsible for keeping your credentials confidential, and you cannot share them with anyone. If you think that your account is compromised or if you lose your credentials, you must immediately reach out to the Customer. The Customer is responsible for managing your accounts, including for blocking, and resetting passwords.

You agree that you can only use Query Identifiers in accordance with the Documentation. You cannot use Query Identifiers to circumvent the number of authorized Identifiers. Each Identifier may only be assigned once per calendar month.

You can configure the Flare Platform to generate alerts, including in the context of the Monitoring Services. You are responsible for following up on these alerts, for determining the appropriate remediation actions and for taking such actions. Any advice provided to you, through the Documentation or otherwise, is only for information.

3. RETRIEVAL FUNCTION

You will only use the Retrieval Function in accordance with applicable laws. You must have the rights to access and retrieve Public Data. You understand that accessing and retrieving Public Data in violation of the foregoing obligations may result in criminal sanctions. Public Data which is retrieved or accessed through the Retrieval Function may contain security issues, harmful content, and stolen properties. Flare will have no liability for Losses resulting from your use of the Retrieval Function in violation of the foregoing.

THE RETRIEVAL FUNCTION ALLOWS USERS TO ACCESS AND REQUEST THE RETRIEVAL OF PUBLIC DATA. THE PUBLIC DATA MAY CONTAIN MALICIOUS CODES, HARMFUL CONTENT, THIRD PARTY IP, AND INDIVIDUALS' PERSONAL DATA. THE PUBLIC DATA IS NOT SCANNED FOR SECURITY ISSUES. POSSESSION OF STOLEN MATERIAL WHICH YOU ARE NOT AUTHORIZED TO ACCESS MAY LEAD TO CRIMINAL INFRACTIONS. YOU MUST HAVE THE RIGHT TO ACCESS AND OBTAIN POSSESSION OF THE PUBLIC DATA THROUGH THE RETRIEVAL FUNCTION. NEITHER FLARE NOR ITS REPRESENTATIVES WILL BE LIABLE FOR ANY LOSSES RESULTING FROM THE USE OF THE RETRIEVAL FUNCTION OR ACCESS TO PUBLIC DATA. FLARE HAS NO CONTROL WHATSOEVER ON

THE PUBLIC DATA. FLARE HAS NO RESPONSIBILITY WHATSOEVER FOR LOSSES RESULTING FROM THE USE OR ACCESS TO PUBLIC DATA.

In other words, you use this function at your own risk. A sandbox and other precautions should be considered.

4. ACCEPTABLE USE

You are not allowed to use the Services in any manner that:

- It is prohibited by applicable laws, including any privacy laws.
- Constitutes the selling, reselling, or commercialization of our IP.
- Will disrupt third parties' use or enjoyment of the Services, including if this use results in automated, constant, and repeated requests for data other than as intended as part of the normal use of the Services, including abnormal usage that overloads servers or causes portions of our network to be blocked (e.g., denial-of-services and distributed-denial-of-service attacks).
- Involves modifying, decompiling, disassembling, deciphering, unencrypting, seeking or otherwise reverse engineering or attempting to reconstruct or discover any source code or ideas or algorithms of any of our Services, and their underlying technology by any means whatsoever, including the Flare Platform.
- Involves scanning, probing, or performing discovery on computer devices, networks, applications and/or other related digital assets for which it does not own or is not fully authorized to perform such actions.
- Involves penetrating our security, including, without limitation, by posting or transmitting files which can contain viruses, worms, Trojan horses or contaminating or destructive features, by circumventing security measures, by attempting to access any part of the Services without proper rights and by manipulating credentials to disguise the origin of content shared through the Services.

Except as intended in the Documentation (e.g., the Retrieval Function), you cannot use extraction methods to extract Content from the Flare Platform, including screen scraping, web scraping, or any other automated or manual techniques for extracting, copying, or downloading data from the Services.

You will not use the Services in a manner that results (a) the creation, transmission, distribution, or storage of material in violation of a third party's IP or in any way that is (b) threatening, abusive, hateful or constitutes or encourages conduct that would be considered a fraud, a criminal offence or likely to give rise to civil liability.

Furthermore, the following restrictions are applicable to the use of the Monitoring Services made available as part of the Services:

- You may only access and use the Services for the Intended Purposes.
- You cannot build profiles on individuals without their consent, or the right to do so, and not for any other purposes than for the Intended Purposes.
- Before monitoring attributes of a person, you can also be required to provide them with a notice. In case of doubts, validate with Customer before profiling someone through search queries.
- You should not rely exclusively on the Services or on any Content obtained from the Services for protecting people against death or bodily harm.

- We may not detect all threats, and the Flare Platform can generate false positives. You are responsible for verifying the information provided, including the Content.
- The risk rating that we provide is approximative based on the data available to us. You should make your own assessment of the risks relating to alerts.

5. IP RIGHTS

The Flare Platform, including any underlying algorithms and technologies, is our IP. Except as we specifically indicate otherwise in the [Terms of Services](#), we do not grant any rights on our IP. You don't have to provide us with any feedback, improvements, or ideas regarding the Services (“**Feedback**”). If you decide to submit Feedback, you understand that we can commercialize them without any compensation due to you.

You can only access and use the Content for the Intended Purposes.

6. CONFIDENTIAL INFORMATION

You agree that you cannot use our Confidential Information, nor any Content obtained through the Flare Platform, for any other purposes than for the Intended Purposes, and that you cannot use or access our Confidential Information, or our Intellectual Property, to build competitive products. Intended Purposes.

Upon termination or expiration of the TOU, or upon Flare's request, you will promptly destroy all copies of our Confidential Information in your possession or control. The obligations in this provision survive the termination or expiration of the TOU.

7. DISCLAIMERS

NOTWITHSTANDING ANYTHING TO THE CONTRARY, AND TO THE FULL EXTENT PERMITTED UNDER APPLICABLE LAWS, FLARE DISCLAIMS ANY AND ALL REPRESENTATIONS AND WARRANTIES, WHETHER EXPRESS OR IMPLIED, REGARDING THE SERVICES, THE DOCUMENTATION, THE FLARE PLATFORM, OR CONTENT MADE AVAILABLE TO YOU THROUGH THE FLARE PLATFORM. YOU ACCESS AND USE THE SERVICES AT YOUR SOLE RISKS.

UNLESS SPECIFICALLY INDICATED OTHERWISE HEREIN, THE SERVICES, INCLUDING THE FLARE PLATFORM AND THE CONTENT, IS MADE AVAILABLE TO YOU “AS IS” AND “AS AVAILABLE”. THE CONTENT MAY NOT BE RELIABLE, TRUE, ACCURATE OR OF QUALITY. WE DON'T REPRESENT NOR WARRANT THAT THE SERVICES WILL BE FIT FOR A PARTICULAR PURPOSE. YOU AGREE THAT, EXCEPT AS REQUIRED BY APPLICABLE LAWS, WE HAVE NO LIABILITY FOR ANY LOSSES THAT YOU INCUR IN RELATION WITH THE TOU OR THE SERVICES.

YOU ARE SOLELY RESPONSIBLE FOR YOUR RESPONSES TO ALERTS, VERIFYING ANY DATA YOU OBTAIN, AND SELECTING APPROPRIATE IDENTIFIERS BASED ON OR IN RELATION TO THE USE OF SERVICES. YOU ALSO ARE SOLELY RESPONSIBLE FOR ANY INSTRUCTIONS, DECISIONS OR ACTIONS TAKEN BASED ON OR IN RELATION TO THE USE OF THE SERVICES. FLARE IS NOT LIABLE FOR RELIANCE ON THE DATA, NOR FOR ANY LOSSES RESULTING THEREFROM. THE SERVICES, INCLUDING THE CONTENT, ARE FOR INFORMATIONAL PURPOSES ONLY AND SHOULD NOT BE CONSTRUED AS LEGAL

ADVICE OR AS A SUBSTITUTE FOR OBTAINING LEGAL ADVICE FROM A QUALIFIED ATTORNEY.

8. LIMITATION OF LIABILITY

TO THE GREATEST EXTENT PERMITTED BY LAW, YOU AGREE THAT FLARE HAS NO DIRECT LIABILITY TO YOU WHATSOEVER, WHETHER DIRECT, INDIRECT OR WHERE APPLICABLE, CONSEQUENTIAL, PUNITIVE, SPECIAL, OR INCIDENTAL, EXCEPT AS SET FORTH IN AN AGREEMENT BETWEEN CUSTOMER AND US. THIS LIMITATION OF LIABILITY APPLIES TO THE FULL EXTENT PERMITTED UNDER APPLICABLE LAWS. WE MAY BE PREVENTED FROM LIMITING OUR LIABILITY UNDER APPLICABLE LAWS, SUCH AS FOR BODILY HARM AND MORAL DAMAGES.

9. SUSPENSION; TERMINATION

Subject to the agreement we have with the Customer, we reserve the right to suspend your access to your account and to the Services with or without notice if you breach the TOU, if we have a reasonable belief that you breached the TOU or you are about to breach the TOU, or as necessary to protect the Services, our Confidential Information, or the Content.

You can terminate the TOU at any time by ceasing to use the Services and requesting the deletion of your account with Customer. We may also terminate the TOU in accordance with our contract with the Customer.

In case of termination or expiration of the TOU, all limitations of liability, exclusions, and provisions, which by their nature should survive the duration of the TOU, will survive. You may not use the Flare IP after the expiration of the TOU.

10. MODIFICATIONS

We reserve our rights to modify the TOU from time to time. We will provide you with a prior written notice of at least 10 days. If you continue to use the Services after this period, or if you otherwise accept the updated TOU, then these modifications will be effective immediately. If you don't agree with the modifications, you can cease to use the Services at any time by requesting the deletion of your account to Customer.

11. GOVERNING LAWS AND JURISDICTION

The governing laws and jurisdiction applicable to the TOU will be as set forth below:

- a) If Customer's registered address with Flare is in Quebec, Canada, the laws of the Province of Quebec, and the applicable laws of Canada, shall govern the TOU, and the parties attorn to the exclusive jurisdiction of the competent courts in the judicial district of Montréal, Quebec.
- b) If Customer's registered address with Flare is elsewhere in Canada, the laws of the Province of Ontario, and the applicable laws of Canada, shall govern the TOU, and the parties attorn to the exclusive jurisdiction of the competent courts in the judicial district of Toronto, Ontario.
- c) If Customer's registered address with Flare is in a country outside of Canada, the laws of the State of Delaware, United States, and the applicable laws of the United States,

shall govern the TOU, and the parties attorn to the exclusive jurisdiction of the competent courts in Delaware, United States.

d) If Customer has negotiated other terms applicable to the TOU's governing laws and jurisdiction, such negotiated terms will prevail over the TOU.

The *United Nations Convention on the International Sale of Goods* is specifically excluded from the application to the TOU.

12. WAIVER OF JURY TRIAL

TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, EACH PARTY TO THIS TOU IRREVOCABLY WAIVES, ANY AND ALL RIGHT TO TRIAL BY JURY IN ANY LEGAL PROCEEDING ARISING OUT OF OR RELATING TO THE TOU.

13. CLASS ACTION WAIVER

TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, EACH PARTY TO THIS AGREEMENT IRREVOCABLY WAIVES, ANY AND ALL RIGHT TO PURSUE OR PARTICIPATE AS A PLAINTIFF OR CLASS MEMBER IN ANY CLASS ACTION OR OTHER CLASS-WIDE PROCEEDING ARISING OUT OF OR RELATING TO THE TOU.

14. GENERAL

The TOU constitute the whole and entire agreement between you and Flare in connection with your use and access to the Services and supersede any other agreement or understanding. The TOU cannot be modified except as set forth herein. Even if we decide not to enforce our rights herein, this will not constitute a waiver of such rights, unless we confirm this in writing. We can assign the TOU upon written notice to you, and our successors and permitted assigns will be bound by the TOU. You cannot assign or transfer the TOU under any circumstances. If it turns out that a section of the TOU isn't enforceable, then that section will be removed or edited as little as required, and the rest of the TOU will still be valid. You can consult the French version of the TOU [here](#).