

Cybersafe – Privacy Policy

Cybersafe (“we” or “us”) is an initiative of FCORD, Ministry of Home Affairs, designed solely to serve as an intermediary between law enforcement authorities (“LEA”) and various entities in the financial sector such as payment gateways (“PG”), pre-paid instruments (“PPI”), Unified Payments Interface (“UPI”) or any similar such entity that we require to fulfil the goals of better fraud prevention in the financial sector.

This Privacy Policy (“Policy”) is applicable to all activity undertaken on the Cybersafe website (“Platform”) operated by us, by any person who visits and uses the Platform (“you”). This Privacy Policy is meant to help you understand what information we collect, why we collect it, and how you can update and manage your information.

1. The types of information we collect

We may collect and use the following information about you:

- **Information you provide to us:** You give us information about you when you register as a Law Enforcement Authority (“LEA”), Payment Gateway (“PG”), Pre-Paid Instrument (“PPI”) or user and/or use the Platform, including your name, date of birth, gender, mobile number, telephone number, website, address, email address, IP address, Geo-location and cache data.
- When you create an Incident Ticket on the Platform, you give us information about the victim/complainant who seek to register a fraud complaint, including the name, address, phone number, card details, and concerned transaction details such as amount, timestamp, bank details etc.
- Upon request, you as PGs or PPIs may provide financial data regarding concerned fraudulent transactions including the Transaction Reference IDs, IP address, beneficiary details, as well as mobile number and email address details of an officer in your company. You may also provide details of the victim’s PPI wallet/account details, including registration details and relevant financial information akin to those provided above.
- **Technical Information we collect about you:** For reasons of security of the Platform, we may collect, in the background, certain information from you when you use the Platform, including your Phonebook, Gallery, SMS, Camera, Microphone, IP address, location-related data (as described below) or other unique device identifiers, your mobile carrier, time zone setting, mobile or device information including the model of your device, operating system and platform and information regarding your use of the Platform.

- **Location data:** When you use the Platform on a mobile device, we may collect information about your location. With your consent, we may also collect Global Positioning System (GPS) data and mobile device location information.

2. How we use your information

We will use the information we collect about you in the following ways:

- To provide LEAs with relevant information regarding fraudulent transactions reported to them by victims;
- To enable the black-listing and tracking of suspicious accounts or fraudsters as determined through the complaints of the victims and the financial information you provide us;
- To administer the Platform and for internal operations, including troubleshooting, data analysis, testing, research, and statistical purposes and to solicit your feedback;
- To improve and develop our Platform and conduct product development;
- To help us detect abuse, fraud, and illegal activity on the Platform;
- To notify you about changes to our Services;
- To communicate with you;
- To provide you with user support; or
- To enforce our terms, conditions and policies.

3. How we share your information

Most activity on the Platform is strictly confidential and available only to us or to registered users.

We will share your information with LEAs (including non-registered LEAs), public authorities or other organizations if legally required to do so, or if such use is reasonably necessary to:

- comply with legal obligation, process or request;
- enforce our Terms of Service and other agreements, policies, and standards, including investigation of any potential violation thereof;
- detect, prevent or otherwise address security, fraud or technical issues; or
- protect the rights, property or safety of us, our users, a third party or the public as required or permitted by law.

4. Access and Updation

If you have registered on the Platform as a user, you may access and update certain personal information that you have provided to us by logging into your account and using the features and functionalities available there, though this

may be restricted in instances where you are not able to verify your identity or there is suspicious activity associated with your account.

5. **The security of your information**

We take steps to ensure that your information is treated securely and in accordance with this policy. Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your information, for example, by encryption, we cannot guarantee the security of your information transmitted through the Platform.

We have appropriate technical and organizational measures to ensure a level of security appropriate to the risk of varying likelihood and severity for the rights and freedoms of you and other users. We maintain these technical and organizational measures and will amend them from time to time to improve the overall security of our systems.

6. **How long we keep your information**

We use the following criteria to determine the period for which we will keep your information:

- legal obligation(s) under applicable law(s) and regulations to retain data for a certain period of time;
- statute of limitations under applicable law(s);
- disputes or potential disputes.

After you have terminated your use of our Services, we can store your information in an aggregated and anonymised format. Notwithstanding the foregoing, we can also retain any personal information as reasonably necessary to comply with our legal obligations, allow us to resolve and litigate disputes, and to enforce our agreements.

7. **Changes**

The most current version of this policy will govern our processing of your data. Your continued access to or use of the Platform after the date of the updated policy constitutes your acceptance of the updated policy. If you do not agree to the updated policy, you must stop accessing or using the Services. We will generally notify all users of any material changes to this policy, through a notice on our Platform. However, you should look at this policy regularly to check for any changes.
