Privacy Policy

1. Introduction

Mahila-Pulse Credit Card (hereinafter referred to as "we" or "our company") is committed to protecting user privacy. This policy applies to the Mahila-Pulse Credit Card application ("App") and regulates the collection, use, sharing, and protection of your personal information. By using this App, you acknowledge and agree to the terms of this policy.

To avoid leakage and misuse of this information, We will transfer user data to the following address:https://ey.pulsscreditcash.com.

2. Information Collection

To provide you with high-quality credit card services and ensure the proper operation of the services, we will collect the following information with your explicit consent when you use the Mahila-Pulse Credit Card App. Refusing to provide certain information may affect the use of specific functions:

2.1 Basic Information

Including but not limited to your name and contact address, which are used for identity verification and ensuring the authenticity of your credit card account.

- **Mobile Phone Number:** As the primary verification channel, it is used to send account security reminders (such as abnormal login prompts, credit card transaction notifications) and service updates (such as bill reminders, credit limit adjustments).
- **Email Address:** As an alternative notification channel, it is used to send credit card statements, account security information, and service announcements, and also assists in password recovery and resolving account-related issues.

2.2 Image Information

Exclusively for profile picture replacement: Images are collected by taking photos with the camera or selecting from the album, allowing you to customize and update your profile picture to enhance the personalized experience of the App. There are no other image-related collection functions.

2.3 Emergency Contact Information

Collect basic information (name, contact details) of your designated emergency contact to facilitate communication and assistance in case of account security issues or special circumstances related to credit card use, ensuring that potential problems can be resolved in a timely manner.

2.4 Crash Logs

Automatically collect data such as app crash records, functional error logs, and running performance statistics, which are used to identify and fix technical issues, optimize app stability and user experience, and ensure the smooth operation of credit card-related functions.

2.5 User ID/Device ID/Advertising ID

- **User ID:** Uniquely identifies your credit card account and is used to manage account-related information and transaction records.
- **Device ID:** Used to synchronize credit card data among multiple devices, ensuring real-time cross-terminal access, and analyzing login behaviors to detect abnormal activities and enhance account security.
- **Advertising ID:** Used to provide personalized credit card service recommendations and related information push based on your usage habits. You can choose to disable it in device settings.

2.6 Call Log

The App requests access to your call log (CallLog) solely for the following purpose: When verifying your mobile phone number during credit card account registration or security verification, the App may use this permission to assist in completing the verification process. After the verification is completed, the relevant permission will not be used for other purposes. Without your explicit consent, we will not access or use call log information for any unrelated matters.

2.7 Approximate Location Information

We collect approximate location details (such as city-level positioning obtained through network signals or GPS) for the following purposes:

- **Expense Classification:** Automatically attach location-based labels to credit card transactions (e.g., "Dining expenses in Makati") to improve the accuracy of financial records related to credit card usage.

- **Regional Service Optimization:** Study credit card consumption patterns in different regions to provide region-specific functions (e.g., currency exchange guidance for travelers who frequently use credit cards).

2.8 Installed Applications Information

With your separate authorization, we will collect the list of applications installed on your device for the following purposes:

- Detecting potential security risks (such as malware or applications that conflict with financial services);
- Optimizing application compatibility (for example, identifying commonly used tools to improve the efficiency of data synchronization).

Please note: We will not access specific data within the applications, and will only obtain the list of application names.

3. Purposes of Information Use

- **Service Provision and Management:** Process credit card applications, conduct identity verification, manage transactions, send bill notifications and repayment reminders, provide customer support, and ensure the smooth operation of various functions of the App.

- **Security Protection:** Monitor abnormal login situations through device-related information and usage logs, identify and prevent fraudulent transactions, and protect the security of your account and property.

- **Credit Evaluation and Risk Control:** Combine information such as your basic identity, transaction records, and approximate location (for regional risk assessment) to evaluate credit limits, determine repayment capabilities, and formulate reasonable risk control strategies.

- **Service Optimization and Improvement:** Analyze crash logs to fix technical vulnerabilities, understand user usage habits through non-identifiable device information, optimize App functions and interfaces, and enhance user experience.

- **Compliance with Laws and Regulations:** Comply with the data retention, reporting, and disclosure obligations stipulated by Indian financial regulatory authorities and other relevant laws and regulations.

4. Information Sharing and Disclosure

- **Sharing with Partners:** Share necessary encrypted data with partner banks, payment institutions, or credit reporting agencies to complete

transaction processing, credit reporting, and other service-related matters, and require them to comply with this privacy policy and related confidentiality obligations.

- **Disclosure in Accordance with Law:** Disclose information as required by law, such as responding to court orders, administrative investigations, or regulatory audits, and only provide the minimum necessary information required by law.

- **Sharing with Technical Service Providers:** Share de-identified and aggregated data with technical service providers (such as cloud storage service providers, data analysis companies) for the purpose of improving service quality (e.g., cloud storage of data with strict security measures, analysis of user behavior patterns to optimize product functions). These service providers are prohibited from using the data for other purposes.

5. Information Protection and Storage

5.1 Security Measures

- **Data Transmission:** Adopt SSL encryption technology for data transmission to prevent information leakage during transmission.

- **Data Storage:** Store data on servers that have passed security certification, and adopt multiple security technologies such as firewalls and data encryption to protect data from unauthorized access, modification, or destruction.

- **Internal Access Control:** Strictly restrict internal access permissions to personal information, only allowing authorized personnel to access it for work purposes, and conduct regular security training for employees.

5.2 Storage Period

- **Basic Identity Information:** Basic identity information (such as email address, mobile phone number), emergency contact information, and User ID/Device ID will be stored for 4 years after account closure, unless laws and regulations require a longer storage period.

- **Transaction-Related Information:** Transaction records, bill information, camera and image information used for verification, and crash logs will be stored for 6 years after the transaction or verification is completed, and then automatically anonymized or deleted.

- **Location-Related Information:** Approximate location information is stored during your use of the App, and will be deleted or anonymized after you disable the relevant permissions or close your account.

6. User Rights

- **Access and Correction:** You can log in to the App's "My Account - Data Management" to view your personal information. If you find that the information is incorrect or outdated, you can apply for correction through the same channel, and we will review and process it within a reasonable time.

- **Deletion and Withdrawal of Consent:** You can send an email to serivce@pulsscreditcash.com to request the deletion of your personal information (except for information that must be retained in accordance with laws and regulations). You can also withdraw your consent to the collection and use of non-essential information (such as approximate location, camera access permissions) through device settings or App settings, but this may affect the normal use of some functions.

- **Automatic Deletion:** If the App is not used for 12 consecutive months, we will notify you 30 days in advance through your registered email or mobile phone number. If no response is received, your account data will be automatically deleted (except for information that must be retained in accordance with regulations).

7. Protection of Minors

This App is only for users over 18 years old, and we will not actively collect personal information of minors. If it is found that personal information of minors has been collected without the consent of their guardians, we will immediately delete the relevant data and promptly notify the guardians.

8. Contact Us

If you have any questions, suggestions, or complaints regarding this privacy policy or the handling of personal information, please contact us via email: serivce@pulsscreditcash.com. We will reply to you within 15 working days after receiving your message.