Agricultural Bank of China Limited
Privacy Policy (for Corporate Customers)
Updated on:September 9, 2020

Preamble

Agricultural Bank of China Limited (registered at No. 69 Jian Guo Men Nei Street, Dongcheng District, Beijing, hereinafter "**we**", "**us**" or "**our**") fully understands the significance of Personal Information to corporate customers (hereinafter "**you**") and to the personal information subjects who represent you in handling businesses (hereinafter "**personal information subjects**"), and will use our best efforts to protect the Personal Information of personal information subjects. We are committed to maintaining your trust in us and will adhere to the following principles to protect the Personal Information of personal information subjects: the principle of parity of authority and responsibility, the principle of clear purpose, the principle of informed consent, the principle of minimization and necessity, the principle of ensuring security, the principle of subject participation, and the principle of openness and transparency, etc. In addition, we undertake that we will adopt appropriate security measures to protect the Personal Information of personal information subjects in accordance with the well-established safety standards in the industry.

This Privacy Policy (for Corporate Customers) (or the "Policy") contains our general provisions on privacy that are applicable to all our products and services for corporate customers. With respect to the specific product (or service), we may also explicitly inform you of the purposes, methods, and scope of our collection and use of the Personal Information of personal information subjects through product (or service) agreements, authorization letters, or other documents, and ensure that your authorization or consent is obtained. Such documents, together with this Policy (for Corporate Customers), constitute the entire privacy policy governing our products and services to corporate customers.

The "personal information subjects" referred to herein includes individuals operating or conducting business for the corporate customers, such as directors, supervisors, senior executives, controlling shareholders, actual controllers of a corporate customer, or legal representative, person-in-chargeor authorized

agents of a corporate customer, etc. (hereinafter "Managers").

Before signing this Policy (for Corporate Customers), you shall convey this Policy to personal information subjects to ensure that they know and fully understand the meaning of this Policy (in particular those sections in bold) and the corresponding legal consequences, and obtain their authorization or consent. If you (including your legal representatives or other authorized agents) click or tick "Agree", you and the personal information subjects conducting businesses for you are deemed to accept this Policy (for Corporate Customers), and we will legally use and protect the personal information of the personal information subjects in accordance with applicable laws, regulations and this Policy.

If you want to know more detailed information, please follow the index below to read the corresponding section:

A. How we collect and use the Personal Information of personal information subjects

Personal Information means all information recorded electronically or otherwise that can be used to identify a natural person or reflect his/her activities, whether on its own or in combination with other data, such as name, birth date, **ID certificate number**, **personal biometric data**, address, **communication and contact details, history and contents of communications, account number and password, financial information, credit information, whereabouts, accommodation**

information, physical health information, and transaction information, etc.

Sensitive Personal Information refers to the Personal Information the disclosure, illegal provision or abuse of which might harm personal and property safety and is very likely to damage personal reputation or physical or psychological health or result in discrimination, specifically, **such as ID certificate number, personal biometric information, bank account, history and contents of communications, financial information, credit information, whereabouts, accommodation information, physical health information, transaction information, and Personal Information of minors aged 14 and under.**

For the purposes set forth below in this Policy, We may collect and use Personal Information that is provided by personal information subjects in the course of using our products or services, is generated as a result of the use of our products or services, or is lawfully collected from third parties in accordance with laws and regulations or your authorization and consent. If we need to collect additional Personal Information about the personal information subjects or use the information we have collected for other purposes, we will notify you in a reasonable manner and seek your consent again before collecting it.

I. Personal Information That You Voluntarily Provide In Connection With Our Core Products And/Or Services

In order to realize the core business functions of all our services for corporate customers (such as online banking platform for enterprises (hereinafter "**online banking platform**"), mobile banking platform for enterprises (hereinafter "**mobile banking platform**"), the counter, bank-enterprise direct association, and bank-enterprise link), we may need to collect Personal Information from personal information subjects. The following is a detailed list of the bank's core business functions and the Personal Information required to be collected in order to realize such functions. **You may not use relevant service if you refuse such collection.** The SMS verification codes and payment codes collected in the following scenarios are used only to verify the identity of the personal information subjects, and the client-side of our system do not store the information.

Please note that if you provide us with personal information subject of others, please ensure that you have obtained the authorization of the personal

information subjects.

1. **Registering, Logging in, and Activating the Public Online Financial Services:**
   (1) In accordance with laws, regulations, and regulatory requirements, when personal information subjects register through online banking platform, mobile banking platform, bank-enterprise direct association, and bank-enterprise link when logging in and activating an account, we will collect their **mobile phone number**, **ID card number**, name and **facial recognition information**, **identity information**, and **communication information**. If the you refuse to provide such information of the personal information subjects, you and the personal information subjects may not be able to successfully register, log in to, or activate the online banking platform or the mobile banking platform, or cannot use our services properly.
   (2) As required by laws and regulations and for security reasons, when a personal information subject registers our online banking platform on your behalf, he/she will be required to provide a **mobile phone number** and send us a text message with a verification code for verification. If the personal information subject refuses to provide a mobile phone number for verification, the registration will be unsuccessful, and the personal information subject will be unable to use relevant functions of products and/or services in our online banking platform. However, a personal information subject may exit the registration/login business and return to the homepage for browsing.
   (3) In order to ensure the account and transaction security of you and personal information subjects, when personal information subjects register, login and activate the mobile bank account through the mobile banking platform on your behalf, we will collect their **mobile phone number**, IP address, MAC address, IMEI, type of the operation system, **communication information**, and network identification information.
   (4) You can authorize personal information subjects to use the mobile banking platform to open an account via video interview. In order to provide this service to you, we need to collect the authorized person's name, **ID card number, and the video image information of the authorized person.**

2. Counter Services:

In the process of providing business services to you through the counter, in order to ensure the security of the services and comply with laws, regulations, and regulatory requirements, we will collect and use the Personal Information related to the business, including the name**,** nationality**, identity information, ID certificate type, ID certificate number, validity period of ID certificate, personal biometric information (facial recognition information) and communication and contact information** of the Manager and the legal representative (responsible person); name, nationality or place of registration, **identity information, ID certificate type, ID certificate number, validity period of ID certificate, valid ID certificate address, and capital contribution information** (currency and method of capital contribution, amount of capital contribution, and shareholding proportion) of shareholders, actual controllers and beneficial owners; and name, gender, nationality, title, educational background, **identity information, phone number, mobile phone number, e-mail address, ID certificate type, ID certificate number, validity period of ID certificate, valid ID certificate address**, and employment status of the senior executives. If personal information subjects refuse to provide such information, you may not be able to normally use our counter services.

3. Smart Teller Machine (STM) Services:

When you authorize personal information subjects to use our STM for business, you may need to provide or authorize us to collect the Personal Information required for relevant services, including the name of personal information subjects, **ID certificate type, ID certificate number, front and back images of ID certificates, settlement card number/account number, fingerprint image, face image, handwritten signature**, and we may also verify the validity of relevant information by verifying **account number/card password**, etc. If you refuse to provide the Personal Information required for certain functions or services, you may not be able to use such functions or services, but this will not affect your use of other functions or services of the STM.

4. Self-Service Equipment Service:

To provide services to you and ensure the security of the services, when you

authorize the personal information subjects to use services on “self-service equipment” (including cash self-service equipment, self-service terminals and queuing calling machines), we may verify the identity of the personal information subjects through **personal image photos, account numbers, passwords, ID certificate type and ID certificate numbers** to help you and the personal information subjects to use the services. If personal information subjects refuse to provide information required for the function or service, you may not be able to use such function or service. Specifically:

(1) Media verification: When you use bank cards or bankbooks to handle business on the self-service equipment, you need to provide us with or authorize us to collect **user information** as required by relevant services, including **bank card number/account number** and **bankbook account number**, and we will verify the validity of relevant information through verification of account **number/card password**.

(2) Facial recognition service: when you use our “self-service equipment” to deposit or withdraw money, transfer funds or use non-card or non-bankbook deposit service through facial recognition services, we will collect the **on-site face image**, **mobile phone number** or **ID certificate type/IDcertificate number** of the personal information subjects for the purpose of verifying the validity of relevant information. We may also need to collect the **payees’ account number** and **account name** when you transfer funds or use non-card or non-bankbook deposit service.

5. Transfer and Remittance Service:

(1) When you use the account transfer and remittance function from our online banking platform or mobile banking platform, we need to collect the **address book information of the personal information subject**, the **registered mobile phone number**, the name, **bank card number, account information, identity information, and communication information of the payees** so that you may use the services.

(2) When you process any single transaction or bulk transactions for business to individuals through the online banking platform or mobile banking platform, we will collect the transferees' name, **account number, account information,**

and identity information.

(3) When you process bulk collection business through the online banking platform or mobile banking platform, we will collect the name, **account number, account information, and identity information of the payers**.

(4) We will collect and preserve the **records of your relevant collection/payment transaction transactions** for your inquiry.

(5) When you or an authorized personal information subject uses the function of transferring funds by face recognition provided by the mobile banking platform, we need to collect the **face recognition information** of the personal information subject as one of the means of payment by password (for transfer verification and sending). You can log in mobile banking platform through your administrator, and enter [More] - [Administrator] - [Face Settings] (enabling the function needs the verification of USB Key, after which the face recognition function will be initiated). After the administrator enters [More] - [the Security Center] - [the Face Password] to record successfully, the face password can be used to conduct the transfer.

(6) When you use the function of transferring funds of your settlement card through the STM, in order to ensure the transaction security, we need to collect the name, **card number, remaining authentication-free amount, transfer amount, transferor's account name and additional security authentication methods** of the payer**.** In order to provide inquiries and convenient transfer service, we need to collect your **transfer records**.

(7) When you use the ABC cheque transfer function through the STM, we need to collect the name, **account number**, and recipient bank information of the payee. In order to ensure the security of the transaction, we need to collect the **mobile phone number** of the Manager. In order to provide inquires and convenient transfer services, we need to collect your **transfer records.** When you use the check transfer preparatory sheet service through the “STM Preparatory Sheet” function of the ABC Micro-service applet, we will collect the **account number** and **account name** of the payee.

In addition, we provide you with a variety of ways to turn off this function. Your administrator can turn off functions via [More] - [Face Settings] when logging in to the mobile banking platform, or via [Settings] - [Operator Information Maintenance] -

[Select the Operator] – [Face Password Switch] when logging in to online banking platform. The operator can also turn off the face transfer function via [More] - [Security Center] - [Face Password] when logging in to the mobile banking platform. But the administrator is still required to conduct the process as described in 5.(5) to re-initiate the face recognition function.

We will collect **facial information** after obtaining your express consent. If you refuse to provide the above information, we will not be able to provide you with the products or services that require facial authentication before their use. With respect to the local biometric authentication functions of mobile terminals of certain brands or models, the facial information will be processed by the mobile terminal provider, and we will not retain any such information generated from the relevant functions of your mobile terminals.

6. Loan Service:

When you apply for a company loan from our online banking platform or mobile banking platform, we will collect the name, **ID card number** of your legal representative (person-in-charge or actual controller), and operator's name, **mobile phone number**, **identity information** and **communication information**.

7. Salary Paying Service:

When you use the online banking platform, bank-enterprise direct association, bank-enterprise link to pay salaries, we need to collect the **bank card number**, name, **mobile phone number**, **account information, identity information and communication information** of your employees (or payees).

You may manage your employees' salaries and wages through the electronic salary list function of the online banking platform, under which circumstances we need to collect the employees' names, **account numbers**, **amount of salary**, **account information**, and **identity information**.

8. Appointment Services:

You or personal information subjects may make an appointment for corporate banking services through the mobile banking platform. In order to provide such service, we need to collect the **geographic location**, name, **mobile phone number,**

ID card number, verification code, **longitude and latitude, International Mobile Equipment Identity Code (IMEI)**, **account information, identification information**, and **communication information** of the personal information subjects in order to provide localized services, location and map functions for them.

You or personal information subjects may make appointments for business and inquire about the application progress through mobile banking platform. In order to provide the service, we need to collect the **mobile phone number**, verification code, **account information, identity information,** and **communication information** of the Manager.

9. Setting up the Administrator:

When you and personal information subjects set up operators through the mobile banking platform, we need to collect the operators' name, **mobile phone number**, **ID card number**, as well as the mobile banking platform **login password, account information, identity information and communication information.**

10. Real-Name Authentication Services:

When you and personal information subjects use the real-name authentication service provided by the online banking platform, you may need to provide personal information subjects' name, **ID certificate type**, **ID certificate number, bank card number/account number**, **face authentication information**, **account information and identity information**. We may also verify the validity of relevant information by verifying the **account number/card password** or by other ways.

11. Mobile Banking Platform Device Binding:

When the personal information subject logs in to the mobile banking platform, he or she will be notified to bind the mobile phone device. During the process, we will collect the unique device identifier of the personal information subject. If the personal information subject refuses to provide this information, he or she will not be able to complete the above binding process.

12. Financial Market Business to Corporate Client:

In the process of your business regarding foreign exchange settlement and sales

to corporations, foreign exchange transactions with corporates, precious metal trading on behalf of Shanghai Gold Exchange, precious metal leasing, precious metal customer derivative, Zhaishibao and corporate customer interest rate swap business through our counter and online banking platform, we may need to collect the name, **ID card numbers**, **contact information**, **communication information**, **account information and identity information** of your directors, supervisors, senior executives as well as the Manager.

13. Investment and Financing Services

When you handle investment and wealth management business via the counter, online banking platform and mobile banking platform, we may need to collect the names, **ID card numbers, contact information, communication information, identity information and transaction information** of your directors, supervisors and senior executives as well as the Manager.

14. International Business Concerning Corporation (Including Domestic Letters of Credit and Financing Thereunder):

When you authorize a personal information subject to conduct international businesses for corporations (including domestic letters of credit and the financing thereunder) via electronic channels such as online banking platform and mobile banking platform, we will collect the names, **account numbers**, addresses of the payees and payers, and the name, **communication information and transaction information** of the personal information subject. We will collect and store your **transaction records** relating to international business concerning corporation (including domestic letters of credit and the financing thereunder) for your inquiry.

II. Personal Information You voluntarily Provided In Relation To Providing You With Additional Business Products And/Or Services

In order to provide you with higher-quality products and/or services, we may need to collect the following information. Your refusal to provide the following information will not affect your normal use of all the above core business functions of our bank, but we cannot provide you with other certain specific functions and services.

You agree that we may use the telephone information provided by you or personal information subjects voluntarily in the scenarios mentioned above to push notices of **promotional events, product advertisements** and other marketing messages to you or personal information subjects via landlines or mobile phones. **If you'd prefer not to receive such marketing messages, you may unsubscribe and reject to receive messages through customer service hotline (95599).**

III. Personal Information That We Proactively Collect And Use To Provide You With Products And/Or Services

In order to comply with the laws and regulations and the basic requirements of the services provided, to ensure the security of your account and system operation, and to prevent fraud through phishing websites more accurately, we will collect information generated during your use of our products or services, so as to determine the risks of your account and control credit risks, ensure the normal provision of our services to you, analyze our system problems, obtain website traffic statistics, and conduct troubleshooting after you send us messages of exceptions. The above information collected by us includes:

1. Log Information:

During your use of our online financial products and/or services for corporate customers, we will automatically collect details about your and personal information subjects' use of our services and save them as network logs, including the language used by you and personal information subjects, your and personal information subjects' visiting time and the webpage records of your and personal information subjects' use of our products and/or services, as well as the operating system, software information, and log-in IP information.

When you deal with business transactions via the counters (Smart Account platform) or STM, your transaction flow logs will be generated in our equipment, which will be saved to our back-end terminal in real-time as the transaction log, regardless of whether your business transaction is successfully completed or not. The specific transaction information recorded shall include **transaction date, transaction time, transaction account number, transaction type, transaction terminal,** and **transaction result**. The basic personal information we record shall include names, **ID**

certificate numbers， communication and contact details of the Manager and the legal representative (or person-in-charge); **names and ID certificate numbers of the shareholders, actual controllers, beneficial owners, and senior executives.**

2. Device Information:

During your use of our online financial products and/or services for corporate customers, for the purpose of ensuring the security of transactions, we may need to obtain personal information subjects' IP addresses, device MAC addresses and operating system types and version numbers.

3. Location Information:

During your use of our online financial products and/or services for corporate customers, we may collect **the location information** of personal information subjects in order to comply with relevant laws and regulations, or to recommend convenient sub-branches to you, or for purpose of helping you use the sub-branch inquiry and sub-branch reservation functions.

IV. Access To Your Device By Our Mobile Banking Platform

In certain scenarios or for certain services, the mobile banking platform may invoke some of your device permissions (See the following table for details). We will ask for your consent individually in a pop-up window before invoking the corresponding permission for the first time. The personal information subjects may choose to disable some or all of the permissions in the settings function of the devices, thereby rejecting us to collect the corresponding Personal Information.

Access to your device	**Applicable scenario/service**	**Purpose of access**	**The consequence of disabling/rejecting access**
Microphone	USB Key, video customer service	Facilitate the use of the audio USB Key and video customer services	video customer service and audio USB Keyare not available
Location	Home page,	Location	Location-related services such as

	nearby sub-branches, sub-branch reservation	Information	current city function, and sub-branch reservation are not available
Bluetooth	Bluetooth USB Key	Your mobile phone can be connected to and interact with third-party devices.	Bluetooth USB Key signature is not available
Camera	Scanning, photo-taking and uploading, video customer service	QR code recognition, face recognition, certificate recognition, account opening reservation	certificate scanning for account opening reservation is unavailable; payment scanning, receipt verification scanning, deposit certificate scanning, video customer service are not available
Album (IOS User Read Only Permission)	Receipt verification, account opening reservation	Photo reading, local device photo scanning and recognition, certificate photo uploading	Account opening reservation, uploading certificate photo, scanning and recognizing local device photo, uploading album photo functions are not available
Save - (only for Android users)	App upgrade, scanning, receipt verification, and account opening reservation	App upgrade, photo reading, code-scanning authentication or certificate photo uploading	App upgrade, local device photo scanning and recognition, photo reading, saving pictures to the photo album are no available
Phone -(only for Android	Login	Obtaining device ID	Not able to log in to the mobile banking platform

users)			

Please note that by enabling these permissions, you or personal information subjects will authorize us to collect and use such information to realize the above functions. If such access is disabled, we will no longer continue to collect or use your and the personal information subjects' information, nor will we be able to provide you with the corresponding functions described above. If we collect or use your or the personal information subjects' information in circumstances other than those mentioned above, we will seek your consent in advance and fully inform you of the purposes, methods, and scope of the information collected and used.

V. Statement On Third Party Service Rules

In order to provide you with better products and services, some of the online finance services for corporate customers you use may be provided directly by third-party service providers in their environments, and we will not collect or share any personal information of personal information subjects with them. **Third parties are not bound by this Policy (for Corporate Customers) and we recommend that you and personal information subjects review the platforms of the third-party service providers and understand how they collect, use, and share personal information of associated persons in accordance with the privacy policies disclosed by them.**

VI. Exceptions To Our Collection And Use Of Personal Information Of Personal information subjects With Consent

In accordance with relevant laws and regulations and national standards, we may collect and use the Personal Information of personal information subjects without your consent, if:

1. **our performance of obligations under laws, regulations and regulatory requirements is involved;**
2. **national security or national defense security is directly involved;**
3. **public security, public health or major public interests are directly involved;**
4. **criminal investigation, prosecution, trial or enforcement is directly involved;**

5. **such collection and use are for the purpose of protecting your or personal information subjects or other individual's life, property and other major lawful rights and interests, where it is difficult to obtain your or personal information subjects or such individual's prior consent;**
6. **such Personal Information is disclosed voluntarily by you or personal information subject to the public, and the collection and use of the information is not in violation of law or our agreement with you;**
7. **such Personal Information is necessary for the execution and performance of the contract upon your or personal information subjects' request;**
8. **such Personal Information is collected from information disclosed through lawful public channels, such as lawful news reports or information disclosure by the government;**
9. **such Personal Information is necessary for maintaining the safe and stable operation of the products or services provided by us, such as for identifying and handling defects in products or failure of services.**

If we collect or use the information of personal information subjects under any circumstances other than those mentioned above, we will fully explain to you the purpose, means, and scope of such collection and use and obtain your prior consent or authorization.

Please understand that the functions and services we provide to you are constantly updated and developed. If the Personal Information of personal information subjects is collected for a certain function or service not mentioned above, we will separately explain to you the content, scope, and purpose of such collection through a webpage alert, interaction process, website announcements or otherwise, and obtain your consent.

B. How we use Cookie and similar technologies

I. Cookie

In order to ensure the normal operation of the websites, we will store small data files named Cookie on your computers or mobile devices, which usually contains identifiers, site names, and certain numbers and characters. Cookies enable the website to verify the information input by personal information subjects (e.g., verification code sent to cellphone), to avoid sending information repeatedly to

personal information subjects (e.g., verification code), and to analyze the number of visitors and the general usage of the website. You may manage or delete Cookies based on your preference. You may remove all the Cookies stored on your computer, and most web browsers have the function of blocking Cookies. However, if you choose to do so, you need to modify your settings each time you visit our websites. The “Help” section in the toolbar of most web browsers will introduce how to prevent your web browsers from accepting new Cookies, how to have your browser notify you when you receive a new Cookie, or how to disable Cookies altogether. In addition, you may deactivate or delete the similar data used by browser add-ons (e.g., Flash Cookie) by modifying the settings of browser add-ons or by accessing the provider's webpage. **However, under certain circumstances, such acts may affect your and personal information subjects’ secured access to our websites and the use of our services.**

II. Web Beacons And Pixel Tags

In addition to Cookies, we will adopt web beacons, pixel tags, and other similar technologies to our websites. For example, our emails to you or personal information subjects may contain the URL linking to our website contents. If you click such URL, we will track your click to better understand your preferences for products or services so as to improve our customer services. A web beacon is generally a transparent graphic image that is embedded into a website or an email. The pixel tags in an email will enable us to learn whether the email is read. You or personal information subjects may unsubscribe at any time if you or personal information subjects prefer not to be tracked in this way by turning off Cookies.

III. Do Not Track

A number of web browsers have the function of Do Not Track, which can send the Do Not Track request to websites. Currently, major organizations developing Internet standards have not yet established relevant policies to specify how websites shall respond to such requests. However, if you or personal information subjects enable Do Not Track on your browser, all our websites will respect your choice.

C. How we store and protect the Personal Information of personal information subjects

I. Our Storage of The Personal Information of Personal Information Subjects

1. The Personal Information we collect and generate within the People's Republic of China will be stored within the People's Republic of China. **However, subject to the authorization or consent from you and personal information subjects, the Personal Information of personal information subjects may be transferred outside the People's Republic of China for the purpose of processing cross-border business, in which case we will comply with the relevant laws, regulations and regulatory rules and take effective measures to protect such Personal Information. For example, before the transfer of cross-border data, we will require overseas institutions to keep the information of personal information subjects confidential by means of execution of agreements, verification or other measures.**
2. We will limit the maximum retention periods of Personal Information of personal information subjects and relevant logs to the extent required by laws and regulations and as necessary for the purpose of this Policy only. Upon the expiration of such retention periods, we will delete or anonymize the Personal Information of the personal information subjects. For example, as for **mobile phone number,** we need to retain personal information subjects' **mobile phone numbers** during their use of our mobile banking platform services so as to ensure their normal use thereof, and we will delete the information after personal information subjects cancel the mobile bank account.

II. Security Measures We Adopt to Protect The Personal Information of Personal Information Subjects

We have adopted security measures in compliance with the industry standards to protect the Personal Information provided by personal information subjects from unauthorized access, copying, public disclosure, use, modification, transmission, damage, or loss. For example, we will use encryption techniques to ensure the confidentiality of the data and utilize trusted protection mechanism to protect the data from malicious attacks, deploy access control mechanisms to strictly restrict access, systematically monitor access to and processing of the information, and ensure that

the Personal Information is accessible only to authorized personnel. Business and development personnel can obtain access to Personal Information only based on the needs of operation and maintenance; the data will be deleted only if authorized by the customer. We will hold training sessions on security and privacy protection to enhance our employees' awareness of the importance of Personal Information protection, and require relevant personnel to execute confidentiality agreements, etc.

If our online financial services for corporate customers ceases in part or as a whole , our relevant products or services will inform you thereof in the form of announcements or otherwise, and we will stop the collection of the Personal Information of personal information subjects by relevant products or services to protect Personal Information of personal information subjects. In the case of interruption of our online financial services for corporate customers, in whole or in part, due to technical failure, network attack, natural disaster and accident, human factor, or otherwise, we will take the emergency response and recovery measures to restore our services as soon as practicable.

Currently, we have completed the evaluation and filing of national classified protection of cybersecurity, and our data center has met the requirements of and obtained the ISO27001 certification in terms of information security.

We will use our best endeavors to ensure the security of Personal Information provided by you. **Meanwhile, please properly keep the account login name, identity information, and other authentication elements (including password and USB-KEY certificate) of you and personal information subjects. Personal information subjects should use complex passwords to assist you in ensuring the security of your account. We will identify the personal information subject with the login name and other identification elements of you and the personal information subject when you use our services. You and personal information subjects may suffer from losses and adverse legal consequences in the case of leakage of such information. If you or personal information subjects become aware that the account login name and/or other identification elements might be or have been leaked, please contact us immediately so that we may take corresponding measures in a timely manner to avoid or mitigate the relevant losses.**

In the case of any Personal Information security incident, we will take effective

remedial measures as required by laws and regulations to prevent its escalation. We will notify you and personal information subjects of such incidents through email, correspondence, telephone, and/or push notification in a timely manner. If it is difficult to notify the personal information subjects, we will publish announcements in a reasonable and effective manner. In addition, we will proactively report to the regulatory authorities, as required, how such Personal Information security incident is handled.

D. How we provide the Personal Information of personal information subjects to third parties

I. Sharing

We will not share the Personal Information of personal information subjects with other companies, organizations, or individuals, except under the following circumstances.

1. Sharing with Authorization or Consent:

After acquiring the authorization or consent from you, we will share the Personal Information of personal information subjects with third parties designated by you within the scope of your authorization.

If we share personal information of the personal information subjects due to our other business needs in addition to the scenarios disclosed in this Policy, i.e., we will expressly notify you of such sharing in accordance with relevant laws and regulations and ask for your authorization and consent.

2. Sharing as Required by Laws:

We may share Personal Information of the personal information subjects with third parties in accordance with laws, regulations, or as mandated by competent government authorities.

3. Sharing with Our Operation Organs and Subsidiaries:

The Personal Information of the personal information subjects may be shared within our operation organs and subsidiaries. We will only share Personal Information within a necessary scope, and such sharing will be subject to the purposes specified herein. The scope of Personal Information to be shared will be subject to specific

business conditions, including the statistical information we submit to regulatory authorities as required, and the personal identity information that we may share within our operation organs and subsidiaries for the purpose of risk management by the group as well as anti-money laundering and anti-fraud purposes. **Once the purpose of processing Personal Information of the personal information subjects is changed, we will ask for your authorization or obtain your authorization and consent again.**

4. Sharing with Partners:

In order to provide you with better and high-qualified products and services, some of our services are provided by our partners. We may share some of the Personal Information of the personal information subjects with our partners to provide better service and create better user experience. We will share your Personal Information only for legitimate, reasonable, and necessary purposes, and will only share Personal Information necessary to provide the services. In addition, we will sign a stringent confidentiality agreement with our partners, requiring them to process the Personal Information of personal information subjects strictly in accordance with our instructions, this Policy, and any related confidentiality and security measures. We will insist that our partners have no right to use the shared Personal Information for any other purpose. **If you refuse to allow us to share with our partners the Personal Information collected that is necessary for the provision of the services, you may not be able to use such services.**

Currently, our business partners include the following types:

When you authorize a personal information subject to register, log in, or use the online financial services for corporate customers, we may share Personal Information of the personal information subject with third-party partners that cooperate with us and provide technical and functional support for us, including third parties that provide us with infrastructure technology services, real-name authentication services, data processing services, etc. For example, we may need to collect **facial image information** from personal information subjects when they register for an account, and share it with our partners providing technology services in order to facilitate the completion of facial recognition, the results of which may be used to assist personal

information subjects in verifying identity and retrieving passwords, etc.

In addition, we will also cooperate with government authorities and platforms, for example, sharing certain Personal Information of personal information subjects with social insurance, customs, tax, and other related authorities. The scope of the sharing of personal information will depend on the specific business situations.

(1) Issuers of the financial products which we sell as an agent:

Such institutions are issuers of the financial products (e.g., funds, insurance and trust) which we sell as an agent. In order to enable you to purchase the above financial products, we may share **the personal identity information**, **personal financial information** (if required by the issuer), **personal account information** and **financial product transaction information** of the personal information subject with the issuers of such financial products which we sell as an agent to the extent as required by such issuers;

(2) Advertising and analysis services partners:

In respect of advertising partners, we may provide them with information relating to its advertising coverage and effectiveness rather than the Personal Information of the personal information subject, or we will anonymize such Personal Information before sharing. To better analyze the usage of our products and services by our clients, we may provide data analysis service providers with the quantity, regional distribution, activeness and other data of our clients, provided that we will only provide such partners with statistic information which will not identify our clients (e.g., 「a 25-year old male in Beijing who prefers to purchase fund investment products」).

(3) Suppliers, service providers, and other partners of technology, consultancy, logistics, and other services:

We may share Personal Information of personal information subjects with third parties that provide services to us, including those providing us with infrastructure technology, data processing, credit review and approval, and customer services, etc. For example,

When you apply for exchanging your credits for commodities on the online shopping mall, we may share personal information subjects' name, **phone number**

and **address** with relevant service providers in order to provide you with services, such as delivery by logistics provider, purchase order inquiry, after-sales service, and customer support;

We may share personal information subjects' name, **email address** or **phone number** with communication service providers as they will send you notifications via email or SMS on our behalf;

We may share the **location data** of you and personal information subjects with map service providers as they require such location data to provide you with map services;

To further facilitate your use of services, we will work with post-loan service agencies and legal service agencies for post-loan management, and we may share personal information subjects' name, **phone number** and **personal credit status** with post-loan service institutions and legal service institutions;

For acquiring services operators, we may provide information necessary for business maintenance services with our outsourcing service providers, including the business' name, **address, contact number**, and the number of terminals used, etc.

5. Co-operation with Third-party Software Development Kit (SDK) Service Providers:

SDK is a compilation of development tools used by software engineers to create applications for the specific software package, software framework, hardware platform, operating system, etc. For the purpose of providing you and personal information subjects with better services, some SDKs are embedded into our mobile banking platform and they will collect personal information subjects' Personal Information in the following scenarios during the use of the mobile banking platform:

Type of SDK	**Name of Plug-in**	**Function and Scenario Description**	**Name of SDK Provider**	**Type of Personal Information**	**Required Access to Your Device**
Circumstances in which Personal Information will be directly collected by SDK					
Map SDK	Baidu Maps and Amap	Providing positioning and map functions	Beijing Baidu Netcom	Longitude and latitude, International	N/A

			Science and Technology Co., Ltd., (http://map.baidu.com/zt/client/privacy/index.html) AutoNavi (https://cache.amap.com/h5/h5/publish/238/index.html)	Mobile Equipment Identity Code (IMEI)	
Data Analysis SDK	Component for our internal data collection	Providing functions of collection and analysis of data from the client-side of our system (user click analytics, mobile phone model, etc.)	Us	User click analytics, mobile phone model, operating system model	N/A
Video Collection SDK	Our Internal Video Collection Component	Account opening reservation - verification of a legal entity's willingness to open an account	Us	User video recordings	Access to camera
Accou	Our	Customer	Us	Mobile phone	N/A

nt Manager SDK	Account Manager Component	service and marketing communications		number, user's gender	
Online Customer Service SDK	Online Service Component	Providing online customer service related services	Us	Mobile phone number, location information, transaction ID, gender, sessionID	Access to the recording function and camera
Other circumstances where SDK collects Personal Information (e.g., we share Personal Information with SDK service providers)					
Identity verification SDK	Our facial recognition component	Transfer and reservation for opening accounts by face recognition	Us	Facial image information	Access to camera
WeChat log-in for sharing SDK	Component for our UMAP sharing	Sharing receipt inquiry results on WeChat	Us	N/A	N/A
Static code scan SDK	Component for our UMAP scanning	Functions of receipt verification and QR code scanning	Us	N/A	Access to camera

We will only share the Personal Information of personal information subjects for lawful, proper, necessary, and specific purposes. We will conclude

confidentiality agreements with stringent terms with the companies, organizations, and individuals with whom we share Personal Information to require them to treat such information in accordance with our instructions, this Policy, and other relevant confidentiality and security measures.

II. Transfer

We will not transfer the Personal Information of personal information subjects to other companies, organizations, or individuals, except that:

1. **we obtain your authorization and consent. We will inform you of the purpose of the transfer of your Personal Information and the type of data recipients. Where any Sensitive Personal Information is involved, we will also inform you and personal information subjects the type of Sensitive Personal Information, the identity of the data recipient and its data security capabilities, and obtain prior express authorization or consent of you and personal information subjects.**
2. **it is required by laws, regulations, or mandatory administrative or judicial requirements; and**
3. **in the event of a merger, acquisition, asset transfer or similar transaction involving the transfer of personal information, we will require the new company or organization in possession of personal information subjects' Personal Information to continue to be bound by this Policy, otherwise we will require the company or organization to obtain your express consent again.**

III. Public Disclosure

We will disclose the Personal Information of personal information subjects to the public only if:

1. we have notified you of the purpose of disclosure of Personal Information and the type of Personal Information to be disclosed; in the case of any Sensitive Personal Information is involved, we have notified you of the content thereof and obtained your express prior consent or authorization;
2. we are required to disclose personal information subjects' Personal Information to the public by laws and regulations, legal proceedings, litigation, or mandatory requirements of governmental authorities.

IV. Exceptions To Authorized Consent

In accordance with relevant laws, regulations and regulatory requirements and national standards, we may share, transfer, and publicly disclose the personal information of personal information subjects without prior authorization or consent from you or personal information subjects if:

1. **our performance of obligations under laws, regulations and regulatory requirements is involved;**
2. **national security or national defense security is directly involved;**
3. **public security, public health or major public interests are directly involved;**
4. **criminal investigation, prosecution, trial or enforcement is directly involved;**
5. **such collection and use are for the purpose of protecting personal information subjects or other individual's life, property, and other major lawful rights and interests, where it is difficult to obtain your or such individual's prior consent;**
6. **the Personal Information is disclosed voluntarily by personal information subject to the public, and the sharing, transfer and public disclosure of the Personal Information is not in violation of law or our agreements with you; and**
7. **such Personal Information is collected from information disclosed through lawful public channels, such as lawful news reports or information disclosure by the government.**

E. How Personal Information Subjects Access and Manage Their Personal Information

In accordance with the relevant laws, regulations, and regulatory rules of China, we guarantee that personal information subjects may exercise the following rights with respect to their Personal Information:

I. Access to Their Personal Information

Except as otherwise provided for in laws or regulations, personal information

subjects have the right to access their Personal Information at our sub-branches, through online banking platform and other means. On online banking platform, the personal information subjects may access to their name, certificate type**, certificate number, telephone number**, user name, **password**, and the **binding mobile phone number** via "Administrator – Setup – Administrator Information Maintenance".

II. Correct and Update Their Personal Information

In the event that personal information subjects become aware of any incorrect input of their Personal Information, they have the right to request us to make corrections at our sub-branches or through online banking platform. In online banking platform, the personal information subjects may correct their name, certificate type, **certificate number, telephone number**, user name, **password**, and the **binding mobile phone number** via "Administrator – Setup – Administrator Information Maintenance". Please note that **the information of your administrator in online banking platform may only be modified or added, and may not be deleted.**

If the personal information subject wishes to update his or her Personal Information, he or she may correct his or her name, certificate type, **certificate number, telephone number**, user name, **password**, and the **binding mobile phone number** via "Administrator – Setup – Administrator Information Maintenance" in the online banking platform.

After the personal information subjects successfully correct and update their personal information in online banking platform, the mobile banking platform will replace the relevant information simultaneously.

III. Delete Their Personal Information

Personal information subjects may request us to delete their Personal Information at our sub-branches under any of the following circumstances:

1. Our processing of Personal Information violates laws and regulations;
2. Our processing of Personal Information is in breach of our agreement with you.
3. You or the personal information subject no longer use our products or services, or the personal information subject cancels his or her account.
4. We no longer provide products or services to you.

IV. Refusal of Our Commercial Advertisements

Personal information subjects have the right to unsubscribe by calling the customer service hotline (95599) the notice of marketing events, commercial electronic information or advertisements, which we send to personal information subjects based on their Personal Information.

V. Change The Scope Of The Authorized Consent

In the part of the business in which the personal information subjects are directly involved, personal information subjects have the right to choose whether to give consent to the collection of their Personal Information through online banking platform. In mobile banking platform, personal information subjects can turn on or turn off the access to location service, access to device information, and making calls through the permission management functions in their mobile phone settings.

VI. Cancellation Of Personal Information Subjects' Accounts (including mobile banking platforms)

The personal information subject may apply for the cancellation of the account of online banking platform at our sub-branches.

Please note that the cancellation of the online bank account by the personal information subject is irreversible. Once the personal information subject cancels the online bank account, the mobile bank account will be canceled simultaneously and we will delete the contracting information in online banking platform and mobile banking platform, unless otherwise specified by laws, regulations, or regulatory authorities in respect of retention period of Personal Information.

Please note that the users registered through our online channels cannot cancel their online banking accounts platform or mobile banking platform accounts simply by closing the online banking platform webpage, uninstalling or stopping the use of the mobile banking platform client-side. The information about you or personal information subjects' online banking platform and mobile banking platform account will not be deleted. You are still required to cancel your account in order to achieve the above purpose.

VII. Respond To The Requests From Personal information subjects

We will reply or respond to such requests from personal information subjects within fifteen (15) business days. **For the purpose of security, personal information subjects may be required to submit their written requests and authorization letter through you, and you may be required to verify the identity of the personal information subject.** Please understand that we may refuse certain requests that are submitted repeatedly in an unreasonable manner, or that require excessive technical means, or that may pose risks to others' legal rights and interests, or that are impractical.

According to the relevant laws, regulations, or regulatory requirements, we may not respond to the request of personal information subjects if:

1. **our performance of obligations under laws, regulations and regulatory requirements is involved;**
2. **national security or national defense security is directly involved;**
3. **public security, public health or major public interests are directly involved;**
4. **criminal investigation, prosecution, trial or enforcement is directly involved;**
5. **we have sufficient evidence to prove that you or the personal information subject have subjective malice or abuse of rights;**
6. **it is for the purpose of protecting the life, property, and other major lawful rights and interests of you, personal information subjects or other individuals, where it is difficult to obtain your or such individual's prior consent;**
7. **our responses to your requests will cause material damage to the legal rights and interests of you, personal information subjects or other individuals and organizations; or**
8. **trade secrets are involved.**

Please note that if we decide not to respond to your requests, we will notify you of the reasons therefor and provide you with the channel for filing a complaint.

F. How We Process Personal Information of minors

Our products, websites, and services to corporate customers are mainly targeted

at enterprises and institutions, and minors are not allowed to open any accounts for corporate customers with us. However, some businesses (for example, the payment business of the online banking platform) may involve the collection of minors' information. If it is found that the Personal Information of a minor has been collected in any business for corporate customers without parental consent, we will try to delete the relevant information as soon as possible.

G. How We Update This Policy

In line with the changes in laws and regulations in China and the needs of our service operation, we will amend this Policy and the related rules from time to time. The documents as amended will supersede all prior documents and take effect immediately after their publication through our online financial service platforms for corporate customers or other channels. Please pay attention from time to time to the changes of relevant contents in relevant announcements, notices, agreements, and rules.

For material changes, we will provide additional notifications in a more prominent manner (including through notifications pushed by APP and sent by email/SMS).

The "material changes" referred to herein include but are not limited to:

1. **material changes in our service modes, such as the purpose of processing Personal Information, the type of Personal Information we process and the way in which we use Personal Information;**
2. **changes of the types of main subjects to which the sharing, transfer or public disclosure of Personal Information is made;**
3. **material changes of you and personal information subjects' rights relating to the participation of Personal Information processing or the way in which such rights may be exercised;**
4. **change of our department responsible for the security of Personal Information processing or of its contact information or complaint channel; and**
5. **high risks as indicated in a Personal Information security impact assessment report.**

You acknowledge and confirm that if you and the personal information

subjects disagree with the updated documents, you and the personal information subjects should immediately cease the use of corresponding services and cancel relevant accounts, and we will cease to collect the Personal Information of personal information subjects; and that you and the personal information subjects will be deemed to have accepted such updated documents if you continue to use the services. You are advised to inform us promptly whenever your contact information changes in order for you to receive our notice in time. We suggest that you promptly contact with us to update the information of the personal information subjects when personal information subjects change, and ensure that the personal information subjects have fully read and understand the content of this Policy (for Corporate Customers).

H. How to contact us

If you have any questions, comments, or suggestions with respect to this Policy, please contact us via the following contact information:

Email: 95599@abchina.com

Customer service hotline: 95599

WeChat public number (Debit card): Agricultural Bank of China

WeChat public number (Credit card): Agricultural Bank Credit Card

Normally, we will respond to questions, comments, or suggestions from you or personal information subjects within fifteen (15) business days upon receipt.

If you or personal information subjects are dissatisfied with our reply, especially if you or personal information subjects think our processing of Personal Information damages lawful rights and interests of you and personal information subjects, you and personal information subjects also have the right to file a complaint to the organizations protecting consumers' rights and interests or to other authorities.