CGB (Guangfa Bank) Personal Banking Account Management Service Agreement

Dear Customer: To safeguard your rights and interests, please read this agreement carefully before signing it, particularly the clauses with bolded titles or text. If you have any doubts or uncertainties about the terms of this agreement or business handling, please consult through our business outlets, CGB APP, official website online customer service, or call CGB's 24-hour customer service hotline at 400-830-8003 for inquiries, opinions, or suggestions.

Article 1: To ensure legal and standard use of personal banking settlement accounts, CGB (hereinafter referred to as "Party A") and the account opener (hereinafter referred to as "Party B", including the account holder, agent, joint account and supplementary card applicants) hereby enter into this agreement based on principles of legality, standardization, equality, voluntariness, honesty, and credit, in accordance with relevant laws and regulations. This agreement shall take effect from the date of signature by both parties and remain valid during the existence of the account opened by Party B at Party A, and shall automatically terminate on the official closure of the account.

Article 2: Applicable laws and regulations of this agreement refer to all currently effective laws, regulations, supervisory policies, supervisory regulations, and requirements of the People's Republic of China (for the purposes of this agreement, excluding the Hong Kong SAR, Macao SAR, and Taiwan region) and their relevant amendments from time to time.

I. Classification of Personal Bank Accounts

Article 3: Personal bank accounts in this agreement refer to personal savings accounts and deposit-type settlement accounts, which are further divided into Class I, Class II, and Class III bank accounts (hereinafter referred to as Class I, Class II, and Class III accounts, respectively).

Class I Accounts: Party A can provide services such as deposits, purchasing financial products including investment and wealth management products, transfers, consumption and payment, cash deposits, and withdrawals through Class I accounts. From December 1, 2016, Party B can only open one Class I account at Party A.

Class II Accounts: Party A can offer services such as deposits, purchasing financial products including investment and wealth management products, limited consumption and payment, limited transfers to non-bound accounts through Class II accounts. Party B can open up to five Class II accounts at Party A. For accounts opened through bank counters or self-service devices and verified in person by Party A's staff, Class II accounts can also handle limited amount cash deposits and withdrawals and transfers into non-bound accounts, and can be issued with physical bank cards. For these accounts, the daily cumulative limit for non-bound account transfers and cash deposits is RMB 10,000 and the annual cumulative limit is RMB 200,000; the daily cumulative limit for consumption and payment, transfers to non-bound accounts, and cash withdrawals is RMB 10,000, with an annual cumulative limit of RMB 200,000.

Class III Accounts: Party A provides services such as limited amount consumption and payment, limited transfers to non-bound accounts through Class III accounts. Party B can open up to five

Class III accounts at Party A, and only one Class III account allowing non-bound account deposits can be opened through electronic channels without face-to-face interaction. For accounts opened at bank counters or self-service devices with in-person identity verification by Party A's staff, transfers into non-bound accounts are allowed; for Class III accounts newly opened through electronic channels without face-to-face interaction, small amount transfers into non-bound accounts are allowed after verification through bound Class I accounts. The balance of Class III accounts at any point should not exceed RMB 2,000; the daily limits of the fund transferred to the Class III non-bound accounts confirmed by staffs face-by-face is RMB 5,000, and annual accumulative limits is RMB 100,000. The daily cumulative limit for consumption, payment, and transfers out of non-bound accounts is RMB 2,000, with an annual cumulative limit of RMB 50,000.

Party A shall open the corresponding account type and provide related services as requested by Party B. When Party B needs to upgrade, downgrade, increase, reduce, or change the service content of the account, they should handle the relevant procedures through the channels provided by Party A, in accordance with the regulations of the People's Bank of China on the classification management of personal bank settlement accounts.

II. Opening and Use of Personal Bank Accounts

Article 4: Party B voluntarily opens a personal bank account at Party A and complies with Chinese financial laws, regulations, supervisory department rules, normative documents, and Party A's business rules. If Party B applies for a debit card, they should also comply with the relevant regulations of China UnionPay and other bank card organizations. If the debit card is used overseas, Party B should also comply with local laws and, if agreements exist between China and the local sovereignty institutions, handle according to these agreements. If Party B handles mobile banking and online banking business, they should also comply with the digital certificate service agreement provided by the electronic authentication service organization.

Article 5: **When Party B applies to open a personal bank account at Party A, they should cooperate with Party A in carrying out customer due diligence according to anti-money laundering laws, regulations, and the People's Bank of China's regulations on the classification management of personal bank settlement accounts. Party B should submit valid identity documents and related personal identity information (name, document number, type of document, validity of the document, gender, nationality, occupation, permanent address or work unit address, contact information, tax residency information, etc.) to Party A. Party B promises and guarantees that the account opening information and identity information provided are true, complete, accurate, legal, and valid, and accepts Party A's review. If there are acts of forgery or fraud, Party B shall bear the corresponding legal responsibilities.**

In cases where Party B's account opening information/reasons for opening an account are doubtful, uncooperative in customer due diligence, unreasonable reasons for opening an account, inconsistency between the business of opening an account and the customer's identity, organized simultaneous or batch account opening behavior, clear reasons to suspect the customer's account opening for card resale or engaging in illegal and criminal activities, or

Party A believes after investigation that Party B's risk of money laundering or terrorist financing exceeds Party A's risk management capabilities, Party A has the right to take measures such as extending the account opening review period, increasing customer due diligence efforts, adding transaction authentication methods, restricting transactions, suspending Party B's non-counter business (non-counter business refers to business channels other than counter channels, such as online banking, mobile banking, WeChat, and other third-party payment channels through Party A's account for consumption and payment, etc.), and if necessary, Party A has the right to refuse to open an account, refuse transactions, or terminate the established business relationship.

If Party B's account is used for illegal platform collections, gambling, telecommunications fraud, and other illegal and non-compliant behaviors, or Party B is suspected of participating in illegal platform collections, gambling, telecommunications fraud, and other illegal and non-compliant behaviors, or in use there are transactions that violate anti-money laundering and other related regulations, suspected money laundering, terrorist financing, proliferation financing, tax evasion, or other illegal activities, or involve sanctions risks, as well as disputes caused by violating relevant legal provisions, Party B shall bear legal responsibilities and compensate Party A for any losses incurred. For the aforementioned behaviors of Party B, Party A has the right to restrict the transaction methods, scale, frequency, etc., of Party B or their accounts. Restrictive measures include but are not limited to transaction blocking, adjusting account transaction limits, suspending non-counter account business, transaction bans, account freezing, etc. After evaluation by Party A, if Party B's risk exceeds Party A's risk management capabilities, Party A may terminate the business relationship when necessary.

Article 6: **When Party B opens an account, Party A will provide supporting transaction media and identity verification methods according to Party B's request. Transaction media include but are not limited to: non-media accounts, debit cards, passbooks, deposit receipts, electronic security authentication tools, etc.; identity verification methods include but are not limited to: the account holder's valid identity document, transaction password, real-name mobile phone verification, biometric features, security verification code, etc.**

Party B should properly keep and use the transaction media and corresponding identity verification methods. The corresponding full identity verification methods of each transaction medium of personal accounts are the proof of identity confirmation when conducting transactions. Any account transactions that meet the corresponding transaction medium and transaction channel are considered legal transactions authorized by the account holder.

Party A's electronic information records generated from transactions processed for the account holder based on identity verification methods are valid evidence for the transaction. Losses caused by loss, disclosure of identity verification methods, or loss, theft, or disclosure of transaction media due to non-Party A reasons shall be borne by the account holder. If the transaction medium is lost, stolen, or verification methods are lost, stolen, or leaked, Party B should immediately handle the oral loss reporting of the corresponding transaction medium and verification method through any means or channels provided by Party A, and Party A will

also stop payment for the account. Party B should personally carry valid identity documents to any Party A outlet within five natural days from the date of oral loss reporting to handle the formal loss reporting procedures. If Party B does not handle the formal loss reporting procedures at Party A's outlet within five days after the oral loss reporting, the oral loss reporting will automatically become invalid, and the losses caused before the effectiveness of the oral loss reporting and after its invalidity will be borne by Party B.

If it is confirmed that Party A has accepted Party B's loss reporting and stop payment request but failed to process stop payment in time, causing financial loss to Party B, Party A shall bear the responsibility. If the original transaction media are found after reporting loss, please bring the media and valid identity documents to Party A's outlet to handle the cancellation of loss reporting procedures. However, if the lost media have been applied for a reissued card or official loss reporting of passbook/deposit receipt, the cancellation of loss reporting will not be accepted. Personal accounts and corresponding transaction media are for personal use by Party B only and should not be rented, lent, or resold; otherwise, any losses incurred will be borne by Party B personally.

Article 7: To meet Party B's account service needs and fulfill Party A's legal obligations to establish account and transaction monitoring mechanisms under the Anti-Telecom and Online Fraud Law, Party B agrees that Party A, under the premise of legal compliance, will inquire and use Party B's name, type of document, document number, mobile phone number, and other related information from legally established telecommunications operators and other units, according to the minimum necessary principle, to obtain information on Party B's mobile phone real-name authentication, mobile phone status, social security payments, etc.

Article 8: Party B promises that the contact phone number retained at Party A is the valid contact phone number used by the account owner themselves, and is an important piece of identity/transaction verification information. There should be no situation where multiple people use the same contact phone number to open and use accounts. **For reasonable situations such as adults acting as agents for minors or the elderly to open accounts and reserve their contact phone numbers, it can remain unchanged after Party B and related parties provide explanations; for batch account openings by employers, reserving financial personnel's contact phone numbers, etc., should be changed to the account owner's contact phone number; for situations where Party B cannot prove the reasonableness, Party A will suspend Party B's non-counter account business according to regulatory requirements. If Party A verifies that Party B's reserved valid contact phone number is a vacant number or unreachable, Party A has the right to take one or more protective measures such as restricting transaction methods, scale, frequency, or suspending Party B's non-counter account business to protect the security of Party B's account and funds.**

Article 9: **Party B promises that any transaction that occurs through verification by the mobile phone number retained by Party B is considered a legal transaction authorized by Party B or themselves, and the electronic information records generated by Party A for transactions conducted for Party B based on the retained mobile phone number are valid evidence for the**

transaction. If the mobile number reserved by Party B is not owned by themselves, or has been stolen, or if there is transaction verification information leakage or a delay in updating their latest mobile number, Party A shall not be liable for the risks and losses of Party B caused by the aforementioned circumstances.

Article 10: **Party A conducts ongoing due diligence on Party B during the business period according to regulatory requirements. Party B must cooperate with Party A to provide relevant identity documents for identity verification. If the identity documents or identity proof documents previously submitted by Party B have expired and have not been updated within a reasonable period (within 90 days from the expiration date) without a reasonable explanation, Party A has the right to suspend business for Party B.**

When Party B's personal identity information changes, they should actively and promptly go to Party A's business outlet or notify Party A through electronic channels and handle the change procedures. If Party B fails to provide true, legal, complete, and valid information to Party A in a timely manner, or Party A re-identifies Party B's identity and finds that Party B's identity cannot be verified, Party A has the right to refuse or suspend services for Party B when necessary. Any losses caused by this will be borne by Party B.

Party B promises to timely notify Party A of changes in contact information, occupation, and residence or workplace address and update them. Party B shall bear the adverse consequences caused by not timely updating information or materials.

Article 11: Party A conducts due diligence on Party B according to legal regulations on tax information due diligence for non-resident financial accounts issued by regulatory bodies. Party B must provide true, timely, accurate, and complete tax residency information to Party A and authorizes Party A to report Party B's non-resident financial account tax-related information to relevant institutions according to national (international) tax reporting requirements. Party A classifies Party B as either a Chinese tax resident or non-resident according to relevant legal regulations.

Tax resident in China refers to an individual who has a domicile in China or does not have a domicile but has resided in China for a cumulative total of 183 days during one tax year. Having a domicile in China means habitual residence in China due to household register, family, economic interests relationships.

Non-residents refer to individuals other than Chinese tax residents. For the rules and taxpayer identification number information on tax residency identification in other countries (regions), please refer to the website of the State Administration of Taxation (http://www.chinatax.gov.cn/aeoi_index.html).

Article 12: **According to relevant regulatory provisions, for Party B who has opened multiple Class I accounts at Party A before November 30, 2016, Party A has the right to investigate and clean up Party B's account situation, requiring Party B to provide explanations and verify the rationality of opening the account. Party B should provide reasonable explanations according to Party A's request. For accounts where the rationality of opening and identity verification cannot be confirmed, Party A has the right to merge accounts or downgrade the account type, etc.**

Article 13: When Party B opens a Class II account through electronic channels without face-to-face interaction, they must bind their personal Class I account or credit card account, and verify personal information consistency through clearing institutions such as China UnionPay to the bank where Party B's Class I account is opened. The verification information should include at least the name of the account applicant, resident identity card number, bound account number (bank card number), reserved mobile phone number of the bound account, and whether the bound account is a Class I account or credit card account, among 5 elements. When Party B opens a Class III account through electronic channels without face-to-face interaction, they must bind their personal account. The verification information should include at least the name of the account applicant, resident identity card number, reserved mobile phone number of the bound account, and account number (card number) of the bound account, etc.

Article 14: **When Party B opens Class II and Class III accounts through electronic channels without face-to-face interaction, they promise that the registered verified mobile phone number is consistent with the mobile phone number used by the bound account and can only be processed with their valid resident identity card original, ensuring the authenticity, legality, and validity of the account opening information and customer identity information.**

When Party A collects and uses the above personal information of Party B for non-face-to-face opening of Class II and Class III accounts within the scope authorized by Party B in electronic channels, the transmission of personal information is encrypted.

For Class II and Class III accounts opened by Party B through electronic channels without face-to-face interaction, during the customer identity continuation period, if Party B does not cooperate with Party A's customer due diligence work and Party A cannot continue to verify, Party A may take measures such as downgrading the account type or restricting transactions, and if necessary, may legally refuse to provide financial products or services. Party B authorizes Party A to handle recharge and withdrawal business for Party B's non-face-to-face opened Class II and Class III accounts and agrees that Party A has the right to use its own payment channels or payment channels of third-party institutions cooperating with Party A for fund transfers. The transaction limits for recharging and withdrawing from Class II and Class III accounts opened non-face-to-face are restricted by payment channels and the limit of the bound account's opening bank, as well as Party A's transaction limit adjustments based on regulatory requirements and protection of fund security.

If the bound account information verification is unsuccessful, account status is abnormal, account balance is insufficient, third-party withholding channel limit adjustments, or due to unforeseeable, insurmountable, unavoidable force majeure factors or other uncontrollable objective factors not caused by Party A, leading to untimely debit or debit errors, failures, Party A will not re-initiate fund collection and payment transactions, and the corresponding consequences will be borne by Party B. If the transaction error or failure is caused by Party B and thereby causes Party A to advance funds, Party A has the right to claim the advanced funds from Party B and has the right to deduct from any deposit in any account opened by Party B at Party A without harming Party B's rights and interests as much as possible. Party B can bind their payment account opened with a third-party payment institution to their personal same-name Class II and Class III accounts.

Article 15: **When Party B opens non-face-to-face Class II and Class III accounts at other banks' electronic channels, binding personal bank Class I accounts opened at Party A, Party A, as the verified bank for bank card account verification business, can receive personal information initiated by Party B voluntarily opening non-face-to-face Class II and Class III accounts at other banks' electronic channels through regulatory-designated clearing institutions (including China UnionPay, the People's Bank of China Clearing Center), and compare it with Party A's retained personal information of Party B for consistency and output verification results, and feed back to the account business verification initiating bank of Party B at other banks. The verification information includes the name of the account applicant, resident identity card number, bound account number (bank card number), reserved mobile phone number of the bound account, and whether the bound account is a Class I account or credit card account, among other elements. At the same time, Party A will retain the log information of this verification business for handling customer complaints and security management for Party B.**

Article 16: When Party B establishes a business relationship with Party A or handles a one-time financial business above the specified amount, they should present true and valid identity documents or other identity proof documents according to anti-money laundering identity verification requirements; if entrusted to others to handle, the agent should also cooperate to provide valid identity proof documents of the agent, and related personal identity information (name, document number, type of document, contact information, etc.), and agree to Party A collecting and retaining photocopies or scanned copies of the identity information and related identity proof documents actively provided by Party B's agent.

Article 17: **To facilitate Party B's online payment, Party B can simultaneously open online quick payment function when opening a personal bank settlement account at Party A face-to-face. For accounts that open this function, the maximum payment limit when signing and binding various third-party payment institutions shall be determined by the agreement between Party A and each third-party payment institution, and Party B can query and adjust by themselves through channels provided by Party A.**

If Party B does not open the online quick payment function through face-to-face, the maximum payment limit for accounts that do not open this function when signing and binding various

third-party payment institutions shall be determined by local regulatory requirements.

Article 18: For the addition of new service functions to personal bank accounts, Party A will provide Party B with business opening and withdrawal choices and announce through official websites, outlets, and other channels.

Article 19: According to relevant regulatory requirements and the need to protect the security of Party B's account and funds, Party A has the right to preset account balance limits, transaction amount limits, and transaction number restrictions for Party B's opened accounts according to factors such as the nature of personal accounts, supporting transaction media, transaction channels, verification methods, etc. Party B can adjust the transaction limits of designated accounts through channels and methods provided by Party A according to actual needs, except as otherwise stipulated by regulatory provisions. Party A will conduct transaction risk reminders according to relevant regulatory requirements or conditions and methods agreed with Party B. Party A provides Party B with various transfer services according to regulatory requirements. When Party B uses non-real-time transfer services, if the funds to be transferred out from Party B's account, including Party B's account, are frozen, temporarily banned, or deducted by public security organs, procuratorates, courts or any other competent authorities requiring Party A to do so, resulting in the failure of the transfer transaction, Party A does not bear responsibility. When Party B applies to open non-counter transfer business, Party A and Party B agree on the daily cumulative limit, number of transactions, and annual cumulative limit for non-counter channels transferring to non-same-name bank accounts and payment accounts. For transfers exceeding the limit and number of transactions, Party B should go to the counter to handle them.

Article 20: When Party B handles personal check business, they should reserve a signature at the bank, and Party A will handle business based on the signature. If Party B loses or changes the reserved personal signature, they should submit a written application confirmed by their signature and go to the account opening outlet to handle confirmation procedures. **It is strictly forbidden to issue blank checks and should not issue checks that do not match the signature or seal reserved in their real name. Otherwise, they will be penalized according to the relevant regulations of the People's Bank of China. If a blank check is issued three times (inclusive) or more within a year, Party A has the right to stop selling checks to Party B.**

Article 21: After Party B has transactions, they can check the account through facilities provided by Party A such as counters, online banking, mobile banking, telephone banking, self-service devices, etc. Party B agrees that Party A reserves the right to reverse wrong transactions.

Article 22: According to the Anti-Money Laundering Law of the People's Republic of China, Anti-Terrorism Law of the People's Republic of China, Anti-Money Laundering Regulations of Financial Institutions, and other anti-money laundering laws and regulations, Party A establishes systems for customer due diligence and keeping customer identity information and transaction records, large transactions and suspicious transaction reporting, etc. Party B should comply with anti-money laundering, anti-terrorist financing, anti-proliferation financing, anti-tax evasion, and other relevant legal and regulatory provisions, as well as Party A's relevant policies, and fulfill

anti-money laundering, anti-terrorist financing, anti-proliferation financing, anti-tax evasion obligations, and cooperate to provide relevant information and materials required for bank account real-name system, customer due diligence, and customer identity information and transaction record keeping. **After the termination of the business relationship between the two parties, Party A should keep Party B's personal identity information for at least 10 years from the year of the end of the business relationship, on the basis of meeting the retention requirements of regulatory bodies for personal customer information.**

III. Change and Cancellation of Personal Bank Accounts

Article 23: Party B can handle Class I, Class II, and Class III account change business through any bank outlet or electronic channel of Party A. When handling changes such as mobile phone number, document validity period, address, etc. for Class I, Class II, and Class III accounts through electronic channels without face-to-face, Party B agrees to re-verify information according to Party A's new account opening requirements and cooperate with Party A to verify the authenticity of personal change information.

Article 24: When Party B cancels an account opened at Party A, they should check the account deposit balance with Party A and return important blank checks and settlement vouchers. **Personal settlement accounts undergoing wage payment, loan deduction, payment agency, and other settlement businesses, as well as accounts with valid contracted fund products, cannot be closed. If Party B does not operate according to the aforementioned regulations, Party A will not bear the losses caused.**

Article 25: Class I accounts, face-signed Class II accounts, and Class III accounts can handle account cancellation through counters or smart machines. Class II and Class III accounts handled through electronic channels without face-to-face can cancel accounts through electronic channels、counters or smart machines. When there are no contracted products, Class II accounts, Class III account balances are zero, no unsettled transactions, and no debts to Party A under Party B’s electronic account, Party B can apply to Party A to cancel the account. If the bound account has been canceled, Party B agrees to re-verify personal identity information according to Party A's new account opening business review requirements, bind a new account, transfer funds from Class II and Class III accounts back to the newly bound account, and then handle account closure.

IV. Personal Bank Account Risk Management

Article 26: **If Party B's account has no transaction records (excluding bank interest accrual) for six consecutive months from the first natural day after the account opening date, Party A has the right to suspend the non-counter channel transactions of the account according to regulatory provisions. Party B must actively provide valid identity proof documents to Party A, and the account business functions can be restored only after Party A re-verifies the identity.**

Article 27: **If Party B’s personal bank account has no active transactions within a year, and the account has no attached foreign currency sub-accounts (including settled) or the balance of**

foreign currency sub-accounts is zero, no attached time deposit sub-accounts (including settled) or the balance of time deposit sub-accounts is zero, then Party A has the right to convert Party B's account into a dormant account. If the account is not activated within two years after becoming a dormant account, Party A has the right to close such accounts. Party B may handle the return of funds and interest after account closure through counters, mobile banking, etc.

Article 28:**Party B shall not rent, lend, sell, or purchase bank accounts, nor use bank accounts to obtain bank credit, nor use accounts opened at Party A for tax evasion, debt evasion, cash withdrawal, money laundering, terrorist financing, proliferation financing, telecommunications fraud, or other illegal and criminal activities. If Party B's account opened at Party A has been identified by public security organs and included in the "involved account" list of the telecommunication network new-type illegal crime ,Party A has the right to take transaction restriction measures for the account opened by Party B according to regulatory requirements. Restriction measures include but are not limited to adjusting account transaction limits, suspending non-counter account business, transaction bans, account freezing, etc.If Party B is identified by public security organs at the municipal level or above as an individual or organization renting, lending, selling, or purchasing bank accounts (including bank cards, the same below) ,Digital Currency Electronic Payment wallet,phone card or payment accounts, etc. or an individual forging others' identities or fabricating agency relationships to open bank accounts, Digital Currency Electronic Payment wallet or payment accounts, Party A will suspend all non-counter business of all bank accounts under Party B's name during the penalty period, but those for tax deductions, social security, water, electricity, and gas fees which are signed by agreement for essential daily living, are excluded.**
When opening an account, Party B should confirm "I fully understand and am clear about the legal responsibilities and disciplinary measures related to renting, lending, selling, or purchasing accounts, and promise to legally open and use my account."

Article 29: If the account opened by Party B and its fund transfers have suspicious transaction characteristics such as centralized inflows and dispersed outflows, Party B should cooperate with Party A to verify the account situation. If Party A still deems the account suspicious after verification or cannot contact Party B, Party A has the right to take transaction restriction measures for the account opened by Party B according to regulatory requirements. Restriction measures include but are not limited to adjusting account transaction limits, suspending non-counter account business, transaction bans, account freezing, etc.

Article 30: To implement regulatory requirements and ensure the security of Party B's funds, when there is risk or abnormality in Party B's account fund transactions, Party B agrees that Party A takes measures such as enhanced identity verification, delayed payment settlement transactions, transaction blocking, adjusting account transaction limits, suspending non-counter account business, transaction bans, account freezing, account closure, etc. After verifying the real intention and background of Party B's fund transactions, Party A should promptly lift Party B's transaction restrictions.

Article 31: If Party B's account is found by Party A or receives a declaration from an individual

whose identity has been misused, and it is confirmed that the bank account was opened under a false name or fake agency, Party A has the right to immediately stop all business of that account and, after obtaining the consent of the misused person or agent, proceed with account closure.

Article 32: When handling business for Party B, Party A legally guarantees the security of Party B's funds and keeps confidential Party B's bank account information (including bank account information, identity information, property information, credit information, financial transaction information, derivative information, and other information obtained and stored during the process of establishing a business relationship with the individual), except for inquiries by public security organs, procuratorates, courts or any other competent authorities, or unless otherwise stipulated by national laws.

Article 33: Party A processes transaction bans, account freezing, etc., for Party B's account according to Party B's active request, other business agreements, or requirements of public security organs, procuratorates, courts or any other competent authorities. When lifting transaction bans or unfreezing accounts, the original transaction applicant or according to related business agreements must submit an application. If Party A operates stop payment, freezing, unfreezing, deduction of account funds, etc., for Party B's account due to Party B's business agreement or requirements of public security organs, procuratorates, courts or any other competent authorities, and disputes consequently arise, Party A does not bear responsibility.

Article 34: **Party A charges personal account management fees and other service fees from Party B according to relevant national laws, regulations, supervisory department rules, normative documents, and the specific content and fee standards shall be subject to Party A's public announcement.**

Article 35: Party A does not bear responsibility for losses to Party B caused by force majeure and unforeseeable, unavoidable, and insurmountable objective situations, which Party A has taken remedial measures but still failed to avoid.

Article 36: **Party B clearly agrees and understands that Party A does not intervene in disputes between Party B and third parties, and Party B should not refuse to pay fees due to Party A on the grounds of disputes with special merchants or third parties.**

Article 37: After Party B completes the opening, changing, or closing of a personal bank account, Party B agrees that Party A records Party B's account information with regulatory bodies according to the requirements of the RMB Bank Settlement Account Management Measures.

V. Protection of Customer Personal Information

Article 38: During the performance of this agreement, for the purposes of establishing, performing this agreement, improving the banking system or business management, and other legal purposes, **Party B agrees and authorizes Party A to collect, store, use, process, and inquire the following personal information provided by Party B during the process of handling this**

agreement or generated by using the service: including name, type of document, document number, document issue and expiry date, gender, country/region (nationality), document address, permanent address, contact phone, profession, tax residency indicator, ethnicity, date of birth, name of the work unit, copies/images of documents, etc. The above information is necessary for Party B to handle business at Party A. If Party B refuses to authorize, it may lead to business handling failure due to non-compliance with regulatory requirements.

Article 39: **Party B understands and is aware that Party A's acquisition of their personal data is mainly used for Party B's account and transaction risk management, identity identification, due diligence, customer classification, provision of products or services, etc.**

Party A legally keeps confidential and promises to take lawful and effective measures to properly store and use all the information and materials provided by Party B, storing and transmitting through professional technical means in encrypted form, and keeping Party B's personal information for the period stipulated by regulatory provisions.

Party A promises to follow the principles of legality, propriety, necessity when using Party B's personal information, and to transmit, process, store, inquire, and use Party B's personal information within the scope, content, and period authorized by Party B. Party A does not disclose, tamper with, damage Party B's personal information, does not sell or illegally provide Party B's personal information to others, and does not inquire or use Party B's personal information unrelated to the provided services or business handling.

Article 40: When Party A processes Party B's sensitive personal information, it will obtain Party B's separate consent confirmation through service agreements or supplementary declarations, except in circumstances where laws and regulations stipulate that consent is not required. For sensitive personal information, Party A will take more stringent protective measures to fully protect Party B's personal information security and legal rights.

Party B voluntarily agrees and authorizes Party A, according to national laws and regulations or for the purpose of performing this agreement to provide services or ensure the security of Party B's account and transactions, to disclose their name, identity card number, bank card number, mobile phone number, transaction information, and other personal information to regulatory bodies, public security organs, procuratorates, courts, or any other competent authorities as necessary.

Article 41: **If Party B is a person without capacity for civil conduct or with limited capacity for civil conduct (especially minors under the age of fourteen), their guardian should carefully read this agreement and use Party A's services or provide information to Party A on the premise of obtaining the guardian's consent. When Party A handles business for Party B, in addition to checking Party B's identity documents, it will also verify the identity documents and guardianship relationship proof documents of Party B's guardian and retain photocopies, scanned copies, or other materials of Party B and Party B's guardian's identity documents and guardianship relationship proof documents that meet regulatory requirements. For situations**

where personal information of Party B is collected with the guardian's consent, Party A will only use and provide externally in circumstances allowed by laws and regulations, explicitly consented by the guardian, or necessary to protect Party B. Party A will protect the confidentiality and security of Party B's personal information according to relevant national laws and regulations. If Party B's guardian does not consent to Party B using Party A's services or providing information to Party A according to this agreement, Party B should immediately stop using Party A's services and notify Party A in time.

Article 42: **Within the scope permitted by laws and regulations, Party B has legal rights related to personal account information. Party B can submit an application to Party A, apply to Party A to handle their relevant personal information through electronic channels such as mobile banking or with valid identity documents at counters, self-service banking, etc., or withdraw consent for Party A to handle their personal account information by closing the account.**

After Party B withdraws consent for Party A to handle personal account information, Party A will no longer handle the corresponding personal account information, but such withdrawal of consent will not affect personal account information processing already carried out. If the information intended to be withdrawn is necessary for Party A to provide services, it should be withdrawn before Party A provides related services or after the termination of related services, except as otherwise stipulated by laws, regulations or regulatory provisions.

Article 43: To ensure that Party B is promptly informed of relevant information on Party A's personal account management, financial information, product services, and other value-added services, Party A may send Party B risk warning information about personal bank accounts, service status notifications, business handling progress and account usage status notifications, market information, investment advice, rights services, product expiration, event invitations, prize redemption reminders, and other reminder information through SMS, announcements, phone calls, APP messages, and other message push methods.

Party B can choose to agree or refuse to receive the above information push services provided by Party A during the account opening process, or unsubscribe according to the unsubscribe method guided by the corresponding information push channel. If Party B clearly provides feedback through confirmation channels such as bank counters, mobile banking, etc., but information push necessary for Party A to provide financial products or services or ensure the safety of Party B's funds and property is excepted. Whether or not Party B agrees to the above authorization does not affect Party A's sending of risk reminders, service status notifications, business handling progress, repayment reminders, and other reminder information to Party B.

After receiving Party B's instruction to refuse information push services, Party A will promptly handle the cessation of information push services for Party B. However, Party B should understand that system modifications need corresponding response procedures and response periods, and system settings may automatically delay effectiveness. Therefore, Party B may still receive push information within a certain period after refusing or unsubscribing from relevant information push services. In this case, Party B can contact Party A by calling Party A's 24-hour

customer service hotline at 400-830-8003 to provide feedback and explanation about the situation, and Party A will further verify and follow up on the feedback issues.

VI. Other Services

Article 44: **A co-branded card refers to a co-branded logo debit card issued jointly by Party A and a third-party institution, applied for by Party B. Once Party B applies for a co-branded debit card, it is deemed as authorizing Party A to apply for third-party institution membership on behalf of Party B. If Party A needs to provide Party B's personal information to the third-party institution for Party B to apply for membership, Party B needs to provide separate authorization confirmation through the relevant co-branded card supplementary agreement. Whether the application for membership with the third-party institution is successful depends on the third party's approval. Party B's application for third-party institution membership not being approved or subsequent membership invalidation does not affect the use of the financial functions of the co-branded debit card.**

Article 45: **A specialty debit card refers to a debit card applied for by Party B and issued by Party A to a specific customer group. After Party B applies for the card, they must separately agree and authorize necessary customer information to the third party through the relevant specialty debit card supplementary authorization form to activate and enjoy specialty rights.**

Article 46: A supplementary card refers to a debit card with certain functions applied for by the main cardholder (Party B) and designated for use by a third person (supplementary card applicant) but attached to Party B's account. To open a supplementary card, the main cardholder (Party B) must apply in person and pass relevant verification. The supplementary card uses funds from the main card account, and the usage limit and period are determined by the main cardholder (Party B). The usage limit of the supplementary card is divided into domestic and foreign currencies, with foreign currency limits converted at real-time US dollar exchange rates. The supplementary card applicant fills out the account opening application form and must be confirmed by the signature of the main cardholder (Party B).

Article 47: A joint account card (hereinafter referred to as co-owned account) refers to an account function provided by Party A for customers (collectively referred to as Party B co-owners), such as family members and business partners, who need to jointly manage funds. Each Party B co-owner of the co-owned account has the same responsibilities, authority, and interests and bears joint and several liabilities for all transactions of the co-owned account. Funds in the co-owned account can be transacted only with the consent of all Party B co-owners. When applying for a co-owned account for the first time, all Party B co-owners must be present together, carrying valid identity documents.

New Party B co-owners can be added to an already opened co-owned account. All original Party B co-owners must be present together and carry valid identity documents, processing the addition of new co-owners with their respective transaction vouchers and transaction verification methods. Deposit business for the co-owned account can be conducted through any possible

channels and forms into the account. Regardless of the method, any deposit business conducted through any debit card and card number corresponding to the co-owned account will immediately be considered as funds in the co-owned account and subject to co-owned account transaction rules after the funds are credited. Transactions using funds in the co-owned account must be conducted through designated transaction channels.

Any business related to funds outflow from the account must be transacted after confirmation by all co-owners of the co-owned account according to the designated transaction channel and verification methods. For counter transactions exceeding the regulatory upper limit, valid identity documents of all co-owners are also required. **If a co-owner of the co-owned account is involved in disputes or cases, causing competent authorities to inquire, freeze, or deduct all or part of the funds in the co-owned account, other co-owners of the account cannot claim any rights against Party A.**

Article 48: The personal bank accounts opened by Party B support the pre-authorization function. According to the requirements of different card organizations, 100%-120% of the funds are frozen during pre-authorization, and the upper limit of the stop payment amount upon completion is 120% of the pre-authorization transaction amount. When conducting pre-authorized transactions overseas, Party B shall bear the exchange rate difference.

Article 49: The debit card opened by Party B at Party A is an IC card, classified by customer level into ordinary, gold, platinum, private banking cards, etc., and by card type into standard, theme, co-branded, supplementary, joint account cards, and other products.

Article 50: **The debit IC card includes a financial main account and an electronic cash application. Electronic cash is anonymous, non-interest bearing, non-loss reporting, only supports RMB settlement, and is used for small-amount consumption by the cardholder. The upper limit of the electronic cash application balance is RMB 1,000 (inclusive); Party B can modify the balance upper limit at the counter of Party A's business outlet, with the same upper limit of RMB 1,000 (inclusive). Party B can load funds into the electronic cash application of their personal debit IC card through self-service channels such as Party A's business outlets, ATMs/CRS, multimedia self-service terminals, etc. Funds in the electronic cash application of Party B's debit IC card are used for small offline transactions without requiring a password during consumption. Funds in the electronic cash application cannot be revoked. Funds from returned goods in the electronic cash application of the debit IC card are refunded to the main account of the debit IC card. The balance of the electronic cash application should be determined based on the electronic cash chip balance. When the debit IC card expires or needs to be replaced due to damage, Party B should return the card for a new one. The funds in the electronic cash application of the original card will be transferred to the main account after 30 days. During this period, the newly replaced card is not allowed to be closed. If the number of electronic cash transactions exceeds the continuous transaction upper limit set by the regulatory body, the transaction should be converted to an online transaction. Funds in the electronic cash application do not verify passwords or check cardholder signatures; any transactions using funds in the electronic cash application are considered to be conducted by**

Party B themselves, and Party B shall bear the risk loss caused by improper storage of the related card (including but not limited to loss or theft). If a transaction has indeed occurred, Party B shall not refuse to pay the transaction amount.

Article 51: Party B can apply for electronic banking services such as mobile banking, online banking, telephone banking, SMS service, etc., at Party A's business outlets with a debit card/passbook and valid identity documents; or they can open and use services provided by electronic banking through Party A's official website (www.cgbchina.com.cn), mobile banking, smart counters, and other self-service channels with the card number/passbook, card/passbook password, and valid identity document number. **Party B should properly keep all important materials and information related to handling electronic banking business, such as identity documents, card number/passbook and its password, mobile soft certificate password, online banking login password, Key shield password, dynamic token, mobile phone number, SMS verification code, mobile banking login password, etc., and should not disclose or hand over to others/unauthorized personnel, and should not leave the above sensitive personal information on untrusted websites or other places to prevent misuse by others. Any losses caused by Party B's intentional or negligent behavior, including failure to properly and cautiously keep the personal sensitive information and being used or misused by others, shall be borne by Party B.** When Party B handles business through electronic banking, they should comply with Party A’s individual electronic banking business-related agreements/charters.

Article 52: If this agreement is signed through face-to-face verification channels, it shall take effect from the date Party A confirms by signature on the application/transaction receipt. If this agreement is signed through various electronic channels, it shall take effect from the date Party A confirms through the system interface (including but not limited to clicking the button under the agreement page agreeing to the content of the agreement, etc.). If any clause of this agreement is confirmed to be invalid, it does not affect the validity of other clauses.

Article 53: If a dispute arises in the process of Party A and Party B performing this agreement, it shall be resolved through negotiation. If negotiation fails, either party may file a lawsuit with the people's court where the settlement account is opened. During the negotiation and litigation period, both parties must still perform the undisputed clauses of this agreement.

Article 54: Party A modifies this agreement according to regulatory requirements or bank management and risk control needs, and makes it public. If this agreement is modified, Party A will announce and inform through business outlets, websites, newspapers, mobile banking, WeChat banking, or other methods conducive to Party B’s acceptance and understanding. During the announcement period, Party B can choose whether to continue using Party A's account; if Party B disagrees with the modification and decides not to continue using Party A's account, they can apply to Party A for account closure. If Party B does not apply for account closure after the announcement period expires, it is considered that Party B accepts the modified content.

Service Content Notes:

1. Debit cards publicly issued by Party A have functions such as savings, consumption, transfer settlement, agency payment, wealth management, pre-authorization, etc., supporting local currency deposit and loan accounts and foreign currency deposit accounts. These cards include standard cards, theme cards, co-branded cards, joint account cards, supplementary cards, social security cards, etc.

2. Party A's contracted CGB wealth management VIP customers need to sign a separate VIP agreement, which may incur account management fees. The fee standards are detailed in Party A's fee announcement, and service details are detailed in the VIP agreement content.

3. Electronic banking security authentication tools (Key shields, soft certificates, etc.) are authentication tools specially held by customers who apply to the bank. Through information technology, they can identify customer identities and transactions and prevent transaction risks.