

Regulations On Provision Of Electronic Banking Services Through Internet Banking

APPROVED
by the Order
of the Chairman of the Board of Directors
SB HSBC Bank Kazakhstan JSC
dated September 03, 2010, No.: w/n

HSBC 
The world's local bank

1. GENERAL PROVISIONS

- 1.1. These Regulations for the provision of Electronic Banking Services through the Internet Banking (hereinafter – the “Regulations”) have been developed in accordance with the current laws of the Republic of Kazakhstan and standards of HSBC Group, and provide the procedure and conditions on provision of Electronic Banking Services through the Internet Banking of SB HSBC Bank Kazakhstan JSC.

2. DEFINITIONS USED IN THE REGULATIONS

- 2.1. The “Bank” – SB HSBC Bank Kazakhstan JSC, including its branches and representative offices.
- 2.2. The “Client” – an individual that has entered into the Agreement and is a Party of this agreement thereof.
- 2.3. The “Agreement” – Personal Electronic Banking Services Agreement, with all amendments and appendixes to it, and any additional terms and conditions for the provision of Electronic Banking Services as published on www.hsbc.kz, through the Internet Banking or available to Client by any other means, any amendments and appendixes to the Regulations for the provision of Electronic Banking Services and any other further instructions or explanation, which appear at www.hsbc.kz or available through Internet Banking from time to time.
- 2.4. The “Authentication” – confirmation of the authenticity and accuracy of completion of an electronic document by using a Security Procedure.
- 2.5. The “Security Code” – is a unique sequence of numeric characters, generated by a special Security Token device issued to the Client by the Bank under the terms of this Agreement, and designated for one-time use when providing access for the Client to Electronic Banking services and for the receipt by the Client of Electronic Banking services. When the Client is trying to access Electronic Banking services for the next time, use of a new unique Security Code is required.
- 2.6. The “Security Procedures” – is a set of organizational measures, as well as software and hardware facilities of the information protection intended for the Client identification when compiling, transmitting or receiving of electronic documents for the purposes of establishment of the Customer right for the use of Electronic Banking services and detection of errors and/or amendments in the content of transmitted and obtained electronic documents, as stated herein.
- 2.7. The “Electronic Banking Services” – services related to the provision by the Bank of banking services to the Client remotely through Internet by the means of Internet Banking.
- 2.8. The “Internet Banking” – a software system, which allows to provide Electronic Banking Services in accordance with the Agreement through Internet, via www.hsbc.kz web portal.
- 2.9. The “HSBC Group” – HSBC Holdings plc, HSBC Bank plc, and its any affiliated companies thereof.
- 2.10. The “Client Dynamic Identification” shall mean the procedure of establishment of the authenticity of the Client for the purposes of unique confirmation of his rights to access an Electronic Banking services by using the Security Code.
- 2.11. The “Client Instruction” – any notice, direction, instruction or information of the Client that is received by the Bank through the Internet Banking with usage of the Client Dynamic Identification and Security procedures.
- 2.12. The “User record” – registration data of the Client in Internet Banking that identify the Client for the purposes of provision of access to the Electronic Banking Services. The User record consists of the Username, answers to the Memorable and Security Questions.
- 2.13. “Username” – Client’s name in Internet Banking that identifies the Client for the purposes of provision of an access to the Electronic Banking Services.
- 2.14. “Memorable questions” – set of questions offered to the Client during accessing Internet Banking, answers to which allow to identify the Client for the purposes of provision of an access to the Electronic Banking Services.
- 2.15. “Security questions” – is a set of questions offered to the Client as an additional identification for the cases stipulated by this Agreement.
- 2.16. Call Center – supporting division of the Bank that carries out the informational and consultancy support to the Bank’s divisions and provides required information to the Clients on Bank’s products and services, and in specified cases an extents, carries out an interactive support of Internet Banking. The volume and content of the required information shall be defined by the Bank independently. The Bank’s Call Center phone number: +7 (727) 259 69 00, operating 24/7.

3. LIST OF ELECTRONIC BANKING SERVICES

- 3.1. Electronic Banking Services provided by the Bank to the Client, include the following:
- 3.1.1. Informational banking services:
- 1) provision of information on User records summary of the Client’s User records opened with the Bank;
 - 2) provision of information on User record balances and transaction history on any Client’s bank User records opened with the Bank;
 - 3) download information to Quicken and Money – software that allows to gather information on the Client’s User records from various financial organisations;
 - 4) enquiry of the Net worth statement on Client’s investments/borrowings;
 - 5) maintaining of the payee lists, including making necessary amendments;
 - 6) payments and transfers history enquiry;
 - 7) saving transfer templates for making similar payments and transfers in the future;
 - 8) interest rates enquiry on the Bank’s products;
 - 9) foreign currency exchange rates calculator reflecting the rates of the Bank for current date and time;
 - 10) update of the Client’s personal information, including the annual income, number of dependants, occupation, employer information, Client’s telephone numbers (home, office, mobile), fax numbers of the Client (home, office), e-mail address, correspondence mailing address;
 - 11) select or hide Client’s User records for interactive session display in Internet Banking;
 - 12) change Memorable questions and answers for the access to interactive sessions in Internet Banking;
 - 13) change Security questions and answers;

- 14) receive credit card statements / advices;
- 15) set up SMS-alerts services for the Client’s User records;
- 16) change SMS-alerts services for the Client’s User records;
- 17) update SMS-alerts delivery settings;
- 18) contact Bank through the channel of secured connections through electronic messages (period and procedure of the Bank’s response are determined by the Bank’s internal procedures);
- 19) receive messages from the Bank.

- 3.1.2. Transactional banking services:
- 1) term deposit User records opening;
 - 2) current User records opening;
 - 3) update deposit’s maturity instructions;
 - 4) making payments and transfers from Client’s User records;
 - 5) currency foreign exchange operations;
 - 6) setting, changing or cancelling special instructions on the Client’s User records;
 - 7) setting instructions on the Client User records for future dated payments and transfers;
 - 8) decreasing of Internet Banking transactional limits, specifically: limits for own User records transfers; bill payments, transfers to pre-designated payees, transfers to non-designated payees.

4. PROCEDURE AND CONDITIONS OF ELECTRONIC BANKING SERVICES PROVISION

- 4.1. Provision of Electronic Banking Services shall only be feasible upon and subject to the conclusion of the Agreement, as well as conducting a registration as a user of the Internet Banking at www.hsbc.kz, and creation of a User record in Internet Banking, Client’s Dynamic Identification and Authentication, in accordance with the Security procedures.
- 4.2. For registration as a user of Internet Banking and creation of a User record, the Client shall obtain Personal Banking Number (hereinafter – the “PBN”), Personal Identification Number (hereinafter – the “PIN”), Security Token Device generating a Security Code (hereinafter – the “Token”).
- 4.3. The Bank shall provide a Token to the Client immediately upon signing of the Agreement, or Token may be sent to the Client by registered mail with notification of receipt, in accordance with the terms and conditions of the Agreement.
- 4.4. PBN and PIN shall be issued to the Client during the personal visit to the Bank, provided that the Client signs the forms of receipt of PBN and PIN, otherwise PBN and PIN may be sent by the Bank to the Client by registered mail with notification of receipt.
- 4.5. For security reasons PBN and PIN may be sent by different mails, or mail operators.
- 4.6. PBN and PIN are required for creation of Client’s User record and are used only during Client’s registration as an Internet Banking user. Further access to Internet Banking will be available by simultaneous use of Username, answer to the Memorable question and the Security Code.
- 4.7. Procedure of the Client’s registration as an Internet Banking user and creation of the Client’s User record:
- 4.7.1. The registration of a Client as an Internet Banking user shall be carried out through Internet Banking by completion by the Client of the required electronic registration forms and conducting certain actions as required during the process of registration as a user of Internet Banking.
- 4.7.2. At the Client’s initial registration as an Internet Banking user, the Client shall input into relevant electronic registration forms PBN, PIN and then create a Username, select a Memorable question from the drop-down menu, type an appropriate answer to the selected Memorable question, then to confirm the answer. The Username and an answer to the selected Memorable question shall be used by the Client for the following access to the Internet Banking. Memorable question shall be individual to the Client, and answer to it shall be easy to remember. PBN and PIN, issued by the Bank shall be used only during initial registration with the following mandatory amendment of the PBN to a Username, individually by the Client.
- 4.7.3. Once a Username and an answer to the Memorable question have been created, the Client shall select two Security questions and input answers to them. The Bank is entitled to suspend or terminate the Client’s access to the Internet Banking and/or provision of the Electronic Banking Services to the Client for the instances when Security questions and answers are repeatedly not completed by the Client.
- 4.7.4. Upon the completion of relevant electronic registration forms and all necessary actions, the Client’s request is processed by the Bank.
- 4.7.5. In case of successful acceptance by the Bank of the Client’s request for registration as Internet Banking user, the Client is notified on the successful completion of registration in Internet Banking. Access to the Internet Banking shall be deemed as a notice on successful registration in Internet Banking.
- 4.7.6. Answers to the Security questions shall be deemed as an additional Client’s identification parameter for the online Internet Banking access reset in case Client’s Internet Banking access is blocked as a result of consecutive incorrect entry (more than three times) of an answer to the Memorable question.
- 4.7.7. The Client shall complete the registration form for the Security Token Device in Internet Banking during the initial access to Internet Banking.
- 4.7.8. Upon completion of the relevant registration form on Security Token Device and completion of all required actions, the Client’s request is processed by the Bank.
- 4.7.9. If incorrect data entered into the registration forms of Security Token Device the Bank has the right to suspend or terminate the Client’s access to the Internet Banking service and/or Electronic Banking Services.
- 4.7.10. Username, answer to a Memorable question, Security Questions and answers created by the Client during registration process, as well as the registered Security Token Device shall be deemed as a Client’s User record for the Internet Banking access.
- 4.8. Upon provision by the Bank of electronic banking services, the Bank keeps confirmation on messages sent and/or received, based on which the Electronic Banking Services are being provided to the Client. Access of the Client to an Electronic Banking Services of the Bank would serve as a confirmation of electronic document receipt by the Bank.
- 4.9. Electronic banking services and/or other additional services shall be paid by the Client in accordance to the Bank’s Tariffs, effective on the day of provision of an Electronic Banking Service and/or another additional service.

5. BLOCKING/UNBLOCKING CLIENT'S USER RECORD AND PBN, PIN, SECURITY TOKEN RE-ISSUE

- 5.1. In case of loss, theft, damage, forfeiture of the PBN and/or PIN and/or Token, Client's User record shall be blocked by the Client's telephone call to the Bank, or by the Client's personal visit to any branch of the Bank.
- 5.2. Once Client's User record in Internet Banking is blocked, Client's access to Electronic Banking Services will be restricted and provision of Electronic Banking Services to the Client will be suspended.
- 5.3. All Client's Instructions received by the Bank through Internet Banking prior to the Client's contact to the Bank for blocking of the Client's User record shall be deemed by the Bank as Instructions properly authorized by the Client.
- 5.4. Unblocking of the Client's User record, except for the cases when Client's User record is blocked as a result of consecutive incorrect input by the Client of answers to the Memorable and/or Security questions, shall be carried out upon receipt of Client's written application in an established by the Bank form, subject to the personal visit of the Client to the Bank, for the purpose of receipt of new PBN, PIN and Token, and further registration as an Internet Banking user.
- 5.5. Unblocking of the Client's User record may also be carried out based on the Client's call to the Call Center of the Bank, subject to the Client's personal visit to the Bank for the purpose of receipt of new PBN, PIN, and Token.
- 5.6. Once unblocking of the Client's User record is carried out, the previous Client's User record will be cancelled. All obligations of the Client to the Bank shall continue to be valid in full until fully fulfilled by the Client.
- 5.7. Repeated receipt of the PBN, PIN and Token, as well as registration as an Internet Banking user shall be carried out in accordance with these Regulations and Agreement.

6. SECURITY PROCEDURES

- 6.1. The security procedures allow to authentically identify the Client and the right of the Client to acquire Electronic Banking Services, reveal misrepresentations and/or amendments in electronic documents content, based on which Electronic Banking Services are provided to the Client, to ensure protection from unauthorized access to the banking secrecy information, and to provide the completeness of such information.
- 6.2. All procedures of information protection shall be fulfilled on the Client's personal computers, through Internet, and at the Internet Banking servers of the Client and the Bank.
- 6.3. For the purposes of keeping confidentiality of information transferred and received in Internet Banking, 128-bit Secure Socket Layer (SSL) Encryption is used with all Personal Internet Banking applications, which is the industry standard encryption used for internet banking. Encryption converts Client's data through Internet Banking into an encoded form before it is sent over the Internet. The encryption helps keep Client's information private between the bank's computer system and Client's Internet browser.
- 6.4. The Client shall carry out a browser check to determine if browser supports 128-bit encryption.
- 6.5. SSL connection allows to detect possible misrepresentations and/or amendments in the content of electronic documents, based on which Electronic Banking Services are provided to the Client.
- 6.6. Protection from unauthorized access to banking secrecy information, and provision of completeness of such information carried out by the means of encryption on several levels with various encryption algorithms within the internal systems and among them. Internet Banking uses firewalls to block potentially destructive information from entering our computer systems and to prevent unauthorised access to the Internet Banking system. Firewall software can be installed on business and home computers as a barrier against hackers and viruses.
- 6.7. To protect Client's computer and account information when using Personal Internet Banking, the Bank uses Digital Certificates to allow Client to ensure the communicating is established with the Bank. During the identification and authorisation of the Client in Personal Internet Banking at the web portal of the Bank www.hsbc.kz, Client's browser challenges the Bank's website to prove its identity using digital certificates. Client's browser can verify the certificate and shall alert the Client if the website does not belong to the Bank. When logging on to the Internet Banking, the Client should always ensure that this identity check has occurred. For instance in Microsoft® Internet Explorer, ensuring that the yellow lock is present on the browser and double-clicking it allows the Client to view the digital certificate of the website that Client's browser has verified.
- 6.8. The Bank uses Server Gated Cryptography (SGC), which allows a browser using 40-bit SSL encryption to function as 128-bit encryption for the duration of the online banking session. This helps to keep Customer online banking transaction information as secure as possible without having to download an updated browser.
- 6.9. Client's remote Internet Banking session is protected in a «secured» environment through Secured Socket Layer (SSL) encryption. SSL technology is used within the remote Internet Banking session to encrypt Client's personal information for keeping confidentiality.
- 6.10. For the identification purposes of the Client during log on to Internet Banking and provision of Electronic Banking Services by the Bank, the following identification data for Internet Banking required: for initial registration – PBN, PIN, following log on – Username, answer to Memorable question, and the Security Code. As an additional Client's identification feature – answers to the Security Questions are used.
- 6.11. During the initial registration of the Client as an Internet Banking user, the Client shall use PBN, PIN and Security Token Device issued by the Bank for the purpose of User record creation and further access to Internet Banking, subject to the registration procedure.
- 6.12. During the Client's initial registration as an Internet Banking system user, the Client shall specify Username, input answer to Memorable question and Security Code within Internet Banking.
- 6.13. The Client shall specify two Security questions and answers to them as an additional Client's identification feature.
- 6.14. Further access to Internet Banking, Client's identification and authentication, as well as provision of

Electronic Banking Services, execution of Client's Instructions shall be carried out only based on the Client's Username, answer to the Memorable question, and Security Code entered by the Client individually during the initial registration (or upon changing the User record) and generated by the Security Token Device. The Security Code shall not be independently amended by the Client.

- 6.15. Upon execution of payments and transfers, and any other actions, execution of which requires a repeated input of the Security Code during Internet Banking session, the Client shall appropriately specify the Security Code as requested by the system.
- 6.16. The Client shall not disclose or provide to any third parties the PBN, PIN, Token, Security Code, as well as answers to Memorable and Security Questions, and is obliged to keep the PBN, PIN, Token, Security Code, and answers to Memorable and Security Questions in a place not accessible by any third parties, ensuring the safekeeping of the integrity and possibility of further usage of PBN, PIN, Token, and answers to the Memorable and Security questions.
- 6.17. In the event of consecutive multiple (more than three times in a row) incorrect input by the Client of an answer to the Memorable question for Internet Banking access and an Electronic Banking Services usage, the Client User record shall be automatically blocked by the Bank unilaterally without additional notification to the Client. Once Client's User record has been blocked Internet Banking access will be suspended, and Client's Instructions will not be executed by the Bank. For unblocking of the Client's User record the Client shall attempt to use the answers to Security questions in accordance with the procedure stated in the Agreement. Unblocking of the Client's User record in the events stated herein may also be made based on the Client's phone call to the Bank's Call Center provided that the Client is identified on the basis of the Bank's internal procedures.
- 6.18. Incorrect input of the Security Code by the Client shall be considered as a basis for non-provision of Electronic Banking Service by the Bank.
- 6.19. Incorrect input of the answers to Security Questions shall be considered as a basis for non-provision by the Bank of Internet Banking access and/or non-provision of Electronic Banking Services.
- 6.20. For Security reasons, Internet Banking has a function of deactivation of the current Internet Banking session of the Client's User record. Deactivation of the Client User record's current session shall mean suspension on provision of Electronic Banking Services in case of Internet Banking session being idle (absence of any operations for more than 10 minutes). To access Internet Banking, the Client shall log on to the Internet Banking again.
- 6.21. For the protection of the Client's personal information that is sent through electronic messages, function of secured electronic mail is applied in Internet Banking that is based on the cryptographic encryption of outgoing messages of the Client and the Bank.
- 6.22. Authenticity of the provision of Electronic Banking Services shall be established as a result of Client's fulfillment of the Security Procedures.

7. SMS-ALERTS SERVICE

- 7.1. SMS-alerts service is an additional feature provided by the Bank to the Client based on the application in a form as established by the Bank through Internet Banking, for the phone number specified in the Agreement, or for the phone number as entered by the Client in Internet Banking system upon SMS-alerts service subscription or amending parameters of SMS-alerts service. The Bank has the right to unilaterally refuse the Client to provide SMS-alert Service.
- 7.2. SMS-alerts service represents a service of the Bank on distribution of messages in form of SMS's on Client's bank account transactions, messages of informational type regarding the Bank's products and any other notifications, as stated in Client's application for SMS-alerts services subscription.
- 7.3. Suspension/termination of SMS-alerts Service by the Client and un-suspension of the SMS-alerts Service:
 - 7.3.1. Suspension/termination of SMS-alerts Service may be carried out by the Client by directly provision of a relevant verbal communication to the Bank through Call Centre, or by filling in the relevant application form through Internet Banking.
 - 7.3.2. Un-suspension of SMS-alerts Service is possible on the basis of the Client's application.
- 7.4. The Bank independently in a unilateral procedure shall define the procedure for delivery, terms of delivery and format of SMS-alerts in accordance with the Bank's internal procedures.

