General Terms and Conditions of Landsbankinn

Landsbankinn hf. | No. 1532-06 | June 2023

1 Introduction

1.1 Scope

The General Terms and Conditions of Landsbankinn (hereafter the Terms/these Terms) apply to transactions between Landsbankinn hf. (hereafter Landsbankinn or the Bank) and a customer. A customer may be a private individual or a legal entity (hereafter legal entity or company). If a customer is not a consumer as provided for by law, special rules, differing from the provisions of these Terms, may apply. In addition to these Terms, contract provisions, terms and rules may apply to specific products or services provided by the Bank. Such provisions shall take precedence over these Terms, in the case of any discrepancies. The Privacy Policy of Landsbankinn shall apply in tandem with these Terms. The Bank's terms and conditions and Privacy Policy are published on its website and are available in Bank branches.

1.2 Changes to the Terms and Conditions

The Bank can at any time make alterations to these Terms unilaterally and without notice. Changes to these Terms are communicated to the customer through messages sent via online banking or with a general notice on the Bank's website or in another manner chosen by the Bank.

If amendments to these Terms involve changes to a master agreement on payment services and are not to the advantage of customers, the amendments shall enter into effect with two months' notice. Notices of amendments to such provisions of the Terms call attention to the fact that customers may notify the Bank of the termination of the master agreement before the changes enter into effect. The customer is considered to have approved changes unless he/she notifies the Bank otherwise before the date of entry into force. If a customer terminates a master agreement before the two months' notice is up yet continues to use the payment account in question or a payment instrument linked to the account after the two months' notice has lapsed, the customer is considered to have approved the changes.

1.3 About Landsbankinn

Landsbankinn provides individuals, corporations and investors throughout Iceland with financial services based on long-term business relationships. The Bank operates branches and ATMs throughout Iceland. The Bank is licensed to operate as a commercial bank in accordance with Act No. 161/2002, on Financial Undertakings, and is subject to supervision by the Financial Supervisory Authority of the Central Bank of Iceland, Kalkofnsvegur 1, 101 Reykjavík, cf. Act No. 87/1998, on Official Supervision of Financial Activities, as subsequently amended (see the Financial Supervisory Authority's website, www.fme.is). Landsbankinn is considered to be the controller of the personal data processed in the Bank's operations in accordance with Act No. 90/2018, on Data Protection and the Processing of Personal Data.

Landsbankinn hf., Reg. No. 471008-0280, Reykjastræti 6, 101 Reykjavík, Iceland
Tel. +354 410 4000. E-mail address: landsbankinn@landsbankinn.is, Website: www.landsbankinn.is. Swift/BIC: NBIIISRE

2 General provisions on the business relationship

2.1 Processing of personal data

Landsbankinn processes its customers' personal data based on these Terms and, as the case may be, agreements, terms and conditions and rules applying to individual products or services the Bank may provide to the customer. The Bank processes all information necessary to fulfil agreements between the customer and the Bank or to take measures at the customer's behest prior to concluding a contractual agreement. The processing of personal data is necessary for the Bank to provide customers with financial services. The Bank may also process personal data based on the customer's consent, law, administrative provisions or based on legitimate interest, as detailed in Landsbankinn's Privacy Policy.

The customer shall provide the Bank with information about his/her name, Id./Reg. No., legal domicile or residence for tax purposes, contact details, as well as other information necessary to the business relationship. The Bank also regularly receives information about customers from third parties in accordance with its Privacy Policy, e.g. information

about registered Id./Reg. Nos., names, marital status, children, legal domicile, residency, place of birth and nationality. The Bank is obligated by law to gather certain information from customers, including laws on measures against money laundering and terrorist financing. For legal entities, the Bank is required to process information, inter alia, about the board of directors, management, persons authorisation to sign for the company and beneficial owners. It may also be necessary for the Bank to process information about its employees, customers or other individuals connected to legal entities. The legal entity is responsible for the accuracy of the information provided to the Bank for the purposes of the business relationship and the legal entity shall ensure compliance with the Data Protection Act in such processing, including ensuring the lawfulness of transmitting such information. It is necessary for the Bank to gather information in relation to customers' applications for loans, other credit facilities or transactions, to monitor lending, transactions and liabilities and for debt collection. The Bank gathers and processes inter alia financial information about customers: (a) from the Bank's own systems, including information about business history, (b) from the registers of current credit bureaus, e.g. Creditinfo lánstraust, such as information from customer surveillance, credit scoring, copy of registered obligations and comparable information, (c) from tax reports submitted to the Directorate of Internal Revenue, (d) from the Register of Enterprises, i.e. a company's registration records, articles of association and comparable information and (e) from partners and processors that work with information about collection and default, such as the Icelandic Banks' Data Centre (RB), i.e. information from a receivables pooling database, and Motus. In the case of default, the Bank may be required to share information about loans and customer liabilities with the aforementioned parties, such as to the registers of Creditinfo lánstraust. Data processors working on behalf of the Bank may receive customers' personal data to carry out transactions or other services on behalf of the Bank. The aforementioned also applies to guarantors and, as the case may be, the customer's spouse.

In order to issue credit, including through self-service channels, the Bank takes automatic decisions on creditworthiness, loan terms and limits as the case may be on the basis of personal profiling of the customer. A customer profile is compiled from personal data the Bank has on the customer, including demographics, information about creditworthiness, i.e. credit rating and category along with the customer's business history.

In order to provide the customer with investment service, the customer's personal data may be shared with domestic or foreign partners involved in the service, custody and/or settlement of transactions, as described in the relevant terms and conditions in more detail.

The Bank also processes personal data on the customer in order to develop and/or introduce tailored products, services or business solutions. For the aforementioned purposes, a needs and target group analysis is prepared, as the case may be on the basis of customer profiles. Personal data must also be processed to ensure the quality of services performed, maintain oversight of customers' standing and for treasury and/or risk management purposes. The Bank contacts a customer for those purposes through such media as email, telephone or messages to mobiles or via online banking or comparable communication channels.

The Bank saves and processes the aforementioned data for the duration of a contractual relationship and after its termination in accordance with law, these Terms, the Privacy Policy, agreements, rules and other terms and conditions of the Bank. The Bank saves copies of customers' identification, including information about the use of electronic ID, the timing and method of identification, and updates the information regularly in accordance with the validity of identification certificates. Refusal by the customer to provide the Bank with personal data or authorisation to process such information may prevent the Bank from providing the customer with requested services.

Phone conversations that lead or may lead to transactions with financial instruments are recorded. Other phone calls between the Bank and customer may also be recorded. Electronic communications between the Bank and customers via email, instant messaging or other chat applications approved by the Bank which lead or may lead to transactions with financial instruments are processed in accordance with legal provisions. Other electronic communications may also be processed. The recording of telephone conversations and processing of electronic communication is intended to ensure traceability and verification of the content of phone calls and electronic communications. The Bank may utilise recorded conversations and electronic communication as evidence should a dispute arise about the subject of communication between parties, e.g. about the prerequisites or implementation of transactions, or to investigate possibly criminal and/or punishable conduct by employees or the customer.

The Bank also processes necessary personal data from customers through the use of cookies, for such purposes as cyber and information security, e.g. by analysing departures from usual customer behaviour. Further information about the Bank's use of cookies is available in the Bank's Privacy Policy. The Bank also processes personal data from the customer's technical environment and to execute business transaction for such purposes as cyber and information security, e.g. by analysing departures from usual customer behaviour. If a customer becomes aware of errors or defects during use of, for example, online banking, app, the Bank's website or other electronic services, the customer must notify the Bank without delay. Resolving errors may require that the Bank logs in to a customer's online banking account.

The Bank's employees are bound by legal obligations of confidentiality concerning any information of which they may become aware in the course of their duties, concerning the business dealings or private concerns of customers. Not withstanding the legal duty of confidentiality towards third parties as regards customer affairs, the Bank is obliged by law to provide public authorities (i.e. regulators, customs, tax and law enforcement authorities) with such information. The confidentiality obligation of employees and parties to which such information is divulged remains even after employment ceases. Any customer who by chance, mistake or without express authorisation receives information that does not pertain to him/her may not record, transmit or take advantage of such information in any way. He/she shall delete the information and notify the Bank that he/she has received such information. The customer shall observe full confidentiality in such instances.

All processing of personal data is in accordance with current data protection legislation at each time. Landsbankinn's Privacy Policy includes a detailed description of the processing and handling of personal data undertaken by the

Bank, including what personal data is processed and for what purpose, the rights of individuals, retention time, sharing of personal data with third parties and security of personal data. The customer has an obligation to familiarise him-/herself with Landsbankinn's Privacy Policy.

2.2 Establishment of a business relationship

A customer enters into a business relationship with the Bank via the Bank's website, online banking, the app or branch/outlet. Upon establishing a business relationship, a customer selects products and/or services and applies for access to online banking. The Bank performs due diligence on new customers by requesting verification of identity and information about them, cf. details in the chapter on Measures against money laundering and terrorist financing. A new business relationship must meet the conditions of these Terms and, as the case may be, agreements, terms and conditions or rules that apply to individual products and/or services. The customer attests, as the case may be, the application, agreement and/or terms in question in accordance with the Bank's requirements at each time. The Bank may, without providing specific grounds, reject an application to establish a business relationship and/or for a product or service, if information is insufficient, the application does not meet the Bank's requirements or for other reasons, as determined by the Bank.

2.3 Measures against money laundering and terrorist financing

The Bank operates in accordance with the Act on Measures Against Money Laundering and Terrorist Financing, as subsequently amended. The Bank is required to perform due diligence on customers, upon the establishment of a business relationship, as part of regular control and/or for individual transactions. To perform due diligence, the Bank calls for, among other details, personal information about a customer, including name, Id. No., legal domicile, job title/position, telephone number, email address, place of birth and nationality, in addition to financial information. Legal entities shall provide information about name, Reg. No., legal address, legal form, board of directors, executive board and person authorised to sign, as well as information about the beneficial owners of the legal entity and persons authorised to oblige the entity. The Bank also gathers information about the origin of the funds customers intend to use in transactions with the Bank, whether transactions are undertaken on behalf of a third party and information about the nature and purpose of the intended business relationship and/or transaction.

As part of due diligence, the customer shall provide proof of identity by showing valid identification issued or attested by a competent authority, e.g. a passport, driver's licence, Icelandic identity card or valid electronic ID. For underage customers, who do not have own personal identification, legal guardians can show their ID. If a business relationship is established on behalf of a legal entity, trust fund or comparable party, all board members, managing director(s) and authorised signatories must verify their identity by showing valid identification. In the case of residents' associations, it suffices that the cashier verify their identity for due diligence purposes. Legal entities prove their identity by providing a certificate from the Enterprise Register of the Directorate of Internal Revenue (Fyrirtækjaskrá ríkisskattstjóra) or equivalent registry as proof of their registration. An assessment shall be made on a case-by-case basis whether to request a copy of a company's Articles of Association and/or audited annual financial statements.

The Bank uses risk-based monitoring of contractual relationships with customers and gathers updates to information as and when necessary, at any time during a business relationship. Under certain circumstances and in addition to the above, the Bank is required to apply enhanced due diligence in certain sensitive cases. In such cases, the Bank reserves the right to request additional information, including personal data, about the customer to carry out enhanced due diligence. If the Bank suspects that the funds the customer intends to funnel into the Bank's systems are earnings from illegal activity and/or linked to terrorist financing, the Bank reserves every right to halt requested transactions without any notice. If the Bank has legitimate grounds or reason to suspect certain transactions of being suspicious with regard to money laundering and/or terrorist financing, the Bank is obliged to report the transaction to the relevant law enforcement authorities and provide all necessary information in connection with the case. Customers are obligated to inform the Bank of any changes to the details submitted to the Bank in relation to due diligence.

2.4 Master agreement as defined by the Act on Payment Services

The provisions of these Terms that fall under the scope of the Act on Payment Services (including provisions on online banking, payment accounts and payment cards) constitute a master agreement for payment service between the customer and the Bank, as defined by the Act on Payment Services.

2.5 Concluding contracts

The customer concludes a binding contract with the Bank and/or confirms his/her approval with a signature to paper, electronic signature, electronic approval, e.g. in online banking, the app or the Bank's website, with a request or approval over the telephone, using a web communication application or via other means of communication, depending on the nature of the obligation at each time and in accordance with the Bank's demands. The customer also attests to the agreements, terms and conditions and/or the Bank's rules specific to certain products or services, as they may be at each time, with his/her reception of such products or services. Non-financially competent minors may confirm their obligation in accordance with above for products and services that do not require confirmation by a legal guard pursuant to these Terms and/or the Bank's rules; contracts for other products and services require confirmation by a legal guardian. If the customer has granted a third party the power of attorney, the proxy obliges the customer with his/her signature.

2.6 Permissions of non-financially competent minors

Contracts between non-financially competent individuals and the Bank for products and services involving financial commitment, require the approval of a legal guardian. A customer who has reached 13 years of age may establish a business relationship and enter into agreements with the Bank for the following, and comparable, products and services without the approval of a legal guardian: Create a payment account for deposit and withdrawal for own

personal income and/or gift funds, manage the account, apply for a debit card for the account and access to online banking and the app. A legal guardian is generally not authorised to withdraw funds from personal income and/or gift funds on the account of a customer who is a non-financially competent minor, unless with the customer's consent. Withdrawals by a legal guardian from accounts of minors are contingent on the authorisation of both legal guardians, where there are two, unless either legal guardian has authorised the other to hold all power of attorney over the account, including authorisation to withdraw funds from the customer's account. A legal guardian may rescind authorisation to make withdrawals from the non-financially competent customer's account. A legal guardian and non-financially competent customer are both authorised to obtain information about the accounts and other transaction of the non-financially competent customer. Landsbankinn must be notified of any changes to the legal guardianship of a minor or the appointment of a legal guardian. The treatment of funds and authorisation of non-financially competent customers are governed by, in addition to these Terms, the Act on Legal Competence and other of the Bank's rules that may provide for conditions additional to these Terms. In accordance with Icelandic law, a customer becomes financially competent at age 18 and becomes the sole custodian of his/her assets. Any authorisations of the legal guardians become null and void at that time.

2.7 Power of Attorney

The power of attorney a customer grants to a third party to represent the customer in dealings with the Bank shall be in writing or in an electric format approved by the Bank, and dated. Power of attorney shall be attested (a) with a hand-written signature or in another manner approved by the Bank and attested by two witnesses, by a lawyer or his/her agent, a certified estate agent or notary public, or (b) signed with a qualified electronic signature or other electronic means approved by the Bank. The power of attorney shall specify the transactions to which it pertains and the customer bears full responsibility for transactions undertaken based on the power of attorney. Should a power of attorney fail to meet the Bank's or legal demands for form and/or clarity, the Bank is authorised to reject any dealings based on it. Agents must provide the same proof of identity as customers. The customer is responsible for notifying the Bank of any changes to a power of attorney. All changes shall be made in writing and meet the same demands for signature and witnesses as the original power of attorney. The changes enter into effect when they are received by the Bank. A power of attorney lacking a fixed term is revoked by the customer. Only the customer can revoke a power of attorney, unless otherwise provided for by law. A proxy may also revoke the authorisations granted to them. A notification of cancellation or revocation of power of attorney must be submitted to the Bank in writing or through other verifiable means, as defined by the Bank, and becomes effective upon registration of the notification by the Bank. The Bank further reserves the right to unilaterally revoke power of attorney if the Bank considers that there is danger of misconduct, fraud, money laundering or similar; if the Bank considers the power of attorney to be insufficient or it has been inactive for over 24 months. Power of attorney automatically becomes null and void upon the demise of the customer or proxy, and upon the cancellation of legal guardianship, deprivation of the financial competency of the customer or proxy. Previously issued powers of attorney remain effective despite the registration of new powers of attorney unless these are specifically revoked. Laws and regulations on granting power of attorney, changing or revoking the mandate apply in other respects.

2.8 Credit transactions and guarantee obligations

Upon initiating credit transactions, the Bank may require customers to provide collateral to guarantee repayment on time and without loss or that a third party guarantee the borrower's obligations or provide collateral. In addition to these Terms, credit transactions are governed by laws, regulations, rules, the terms and conditions of the relevant product or service, the terms and conditions of the relevant debt instrument and/or guarantee obligations and any other rules of the Bank that may apply. The Bank reserves the right to deny a customer credit.

2.9 Information provision

The Bank sends messages to customer, information and notifications about banking business through online banking or the app or via other communication channels determined by the Bank at each time. The Bank may also use physical post/email in exceptional cases. The fee for postal service is listed in the Bank's tariff. The Bank sends push notifications to the customer via online banking and the app. The customer can change default settings for push notifications in his/her smart device and computer browser. If the customer wishes to change his/her contact details, i.e. phone number or email address, he/she shall update this information in online banking, the app, with the Bank's Customer Service Centre or at a local branch.

To log in to online banking/the app, the customer shall always do so through the Bank's website or open the app through means provided by the Bank and identify/authenticate in a secure manner, in accordance with the Bank's requirements. The customer shall show enhanced precaution as regards false messages, such as text messages or emails that include links to purported log-in pages for online banking/the app, which the customer may receive from a third party, for such purposes as gaining access to personalised security credentials and/or defraud the customer. The Bank does not send customers messages with links to log in to online banking/the app. The Bank may send to customers messages that include links following customers' requests to access certain of the Bank's services. The message from the Bank will refer to the requested service. If the customer receives a message that includes a link, without having previously requested a specific service from the Bank, the message is fraudulent and the customer shall not click on the link, reply to the message or authenticate him-/herself as the message requests. Customers shall familiarise themselves with the Bank's instructions and guidelines for security measures and follow them in all respects.

2.10 Interest

Interest rates on deposits and loans are subject to change unless otherwise stated or agreed. Deposit and lending rates are determined and amended without prior notice in accordance with the Bank's current tariff. If the Bank has agreed to fixed interest rates or other special interest terms, interest rate changes are subject to the terms of the

agreement between the Bank and the customer. Information about the Bank's deposit and lending rates are available on the Bank's website, from its Customer Service Centre and in branches. In calculating interest, each month shall be considered to have 30 days and each year to have 360 days, unless otherwise agreed. Interest appears on annual statements available through online banking or other electric means at the beginning of each year. Interest on outstanding debt and inflation-indexation is debited monthly unless otherwise agreed. Lending interest varies according to the type of loan. Unless otherwise agreed, interest is calculated on loans as of the first payment date.

A banking day is a weekday when Landsbankinn's general branches are open. If a due date, which is also the final date for payment, falls on a weekend or public holiday it shall be moved to the following banking day. If the due date and final date for payment on claims in collection by the Bank for a third party do not coincide, the final date for payment shall not be moved even though it falls on a weekend or public holiday.

These Terms include a section on payment accounts which contains special provisions for interest on payment accounts.

2.11 International transactions

Landsbankinn shall bear no responsibility for possible mistakes or negligence resulting from its customer's choice of foreign business partners and their reliability. The same applies to mistakes or negligence on behalf of foreign financial undertakings. The customer is advised to familiarise him-/herself with the terms and conditions of the foreign financial undertaking, as well as current legislation and business conventions of the state in question. Landsbankinn's exchange rates apply to all foreign currency transactions, unless expressly agreed otherwise. The nature of the transaction determines the rate used, be it spot rate, closing rate or a special rate determined by the Bank. Any risk of resulting trading gains/losses shall be borne by the customer, unless otherwise expressly agreed.

These Terms contain special provisions for payment accounts and foreign currency payments.

2.12 Tariff

The customer pays charges for the Bank's products and services and other expenses linked to services rendered in accordance with the Bank's tariff at each time. Should other terms or the Bank's agreements with the customer provide for charging fees, those terms shall take precedence over the Bank's tariff. The Bank is authorised to debit fees and costs from the customer's payment account with the Bank and such direct debit shall appear on account statements. Landsbankinn may change its tariff without notice. Landsbankinn's tariff is available on the Bank's website, www.landsbankinn.is. The customer can also access information about the tariff in branches or from the Bank's Customer Service Centre.

3 Online banking

3.1 General information about online banking

Online banking is website that Landsbankinn's customers log in to using verification/authentication methods approved by the Bank. Online banking is accessible from the Bank's website, through mobile banking and the app. In order to take advantage of online banking services, the customer must have equipment that is linked to the Internet. The Bank reserves the right to unilaterally determine what services and communication channels are offered via online banking, and to alter those services/communication channels. Online banking services may vary according to whether the customer logs in through the Bank's website, mobile banking or the app. Landsbankinn owns the software used in online banking. The customer is authorised to access and use it. The customer is completely prohibited from making alterations or having alterations made to software connected with online banking.

Personalised security credentials are personalised components, such as PIN, security number, passwords, security codes, unique identifier numbers/codes sent to the customer to confirm transactions, approved by the Bank at each time for customer verification/authentication. Verification/authentication is a method that allows the Bank to verify the customer's identity or confirm authority to use a specific payment instrument, including the use of personalised security credentials. Strong customer authentication is verification based on two or more components classified as knowledge, possession and behaviour. The Bank reserves the right to amend its verification/authentication requirements without notice. Once the customer has logged in to online banking, the customer is responsible for and obliged by all actions carried out in online banking. The same applies if a third party gains access to information about access to online banking or is able to access it in another manner. The customer is responsible for adequately ensuring the safety of personalised security credentials he/she uses for verification/authentication. The customer is prohibited from granting third parties access to his/her personalised security credentials and shall at all times ensure that no-one can get their hands on, see or copy the customer's personalised security credentials. The customer shall keep secret his/her personalised security credentials and all information relating to his/her verification/authentication for online banking and information linked to payment instruments (such as payment card numbers) and is responsible for ensuring that such information is neither divulged nor accessible to unauthorised parties. The customer shall show enhanced precaution as regards false messages, such as text messages or emails that include links to purported log-in pages for online banking/the app, which the customer may receive from a third party, for such purposes as gaining access such information, including to personalised security credentials and/or defraud the customer. Should the customer fail to safeguard personalised security credentials and other aforementioned information securely or in accordance with the above, such as fail to show precaution with respect to false messages from a third party, this shall constitute gross negligence by the customer. Should the customer become aware that an unauthorised party has attempted to gain or acquired knowledge of the customer's personalised security credentials and other aforementioned information, the customer shall notify the Bank without delay and, as the case may be, alter his/her personalised security credentials. The same applies if a customer becomes aware of loss, theft or misuse of a payment instrument or unauthorised use thereof. To ensure safety, the customer shall activate locking mechanisms on

the equipment he/she uses to log in to online banking. The Bank shall not be responsibility for damages caused by use of online banking or the use of connections to online banking. Nor shall the Bank bear responsibility for loss the customer suffers as a result of a third party gaining access to personalised security credentials, access to accounts in online banking/the app, e.g. through the aid of false messages, or access to information about a payment instrument (such as payment card numbers). The Bank shall not be liable for any direct or indirect damage which may be caused by the suspension of online banking, links or additions to online banking without prior notice, for instance, due to necessary maintenance actions, malfunction of software or hardware, system modifications, or other circumstances beyond its control. If the customer lends, sells or authorises a third party to access a device on which the app has been installed, he/she is obliged to log out of the app first. If the device has been tampered with in a manner that compromises its security in any way, for instance, with the installation of insecure applications, use of the app on that device is no longer secure and thus prohibited. The customer shall show caution in the use of online banking. If the customer is sent a unique identifier number/code to approve a payment transaction, the customer shall not authorise the payment with the number/code unless they have ensured that the amount, currency and recipient are correct. Failure by the customer to uphold precautionary obligations in accordance with the above is considered gross negligence on behalf of the customer.

The customer shall notify the Bank without delay if he/she becomes aware of misuse or unauthorised use of online banking. The customer shall not be suffer the damages caused by use of online banking if the Bank fails to take appropriate steps as provided for in the Act on Payment Services, due to notification obligations linked to payment instruments that have been lost, stolen or misused. The Bank may, without prior warning or notice, terminate the customer's access to online banking or limit the customer's access to online banking in part or in whole, temporarily or permanently, in the following instances: (a) if there is a suspicion of unauthorised or fraudulent use of online banking or services in online banking, (b) if there is a suspicion of breaches of the Bank's rules or terms and conditions, (c) if there is a suspicion that a third party may have gained access to the customer's access information, with our without the customer's consent, (d) due to file and system updates and changes or other technical or security reasons, or (e) if the customer's estate enters into bankruptcy proceedings or the customer seeks composition, payment moratorium, or if other similar conditions exist. The customer is notified as soon as practicable. If the reasons for termination are removed, the Bank shall grant access again. The Bank is authorised to terminate the customer's access to online banking if the customer's account has been inactive over a 6-month continuous period or longer. Information about transactions, including the status of transaction orders, may be temporarily inaccessible in online banking due to a heavy load on the relevant computer and trading systems. Certain services or actions in online banking mat determine device location based on GPS coordinates, network systems or phone company distribution systems, including information about service points. Access to such services can be controlled through each devices' settings. The Bank does not retrieve location information from the device without clear authorisation. The Bank shall not be responsible for invoices that appear on the list of unpaid invoices and where the Bank is not the invoicer. Any objections the customer may have to such invoices shall be directed at the registered invoicer.

3.2 Special provisions for online banking for corporates

An application for corporate online banking, approved by Landsbankinn, and these Terms constitute an agreement for corporate online banking. The persons authorised to oblige a company under its rules or according to the Registrar of Limited Companies (board of directors, CEO or authorised signatory) shall notify the Bank of the users who are to be granted access to online banking and set out the extent of their access authorisations. The authorised signatory and CEO as recorded in the Registrar of Companies are access control managers in corporate online banking. A company can also assign the role of access control manager to a user who then has full and unlimited access to the company's online banking account, including the authority to view all actions in online banking. The access control manager has authority to assign access authorisation to other company employees in online banking at any given time and to determine the scope of each access authorisation. If the company does not designate an access control manager, the person who registers the company becomes access control manager by default. Users receive access information to their online banking. Companies shall ensure that users are acquainted with these Terms and are aware of the responsibility resting on the company as a result. Once the user has logged in to online banking using his/her verification/authentication, the company is responsible for and obliged by all actions undertaken in online banking. The access control manager and users may not be on a default registry as the subject of unsuccessful attachment or bankrupt. Access control managers and users who have authorisations exceeding viewing and batch entry must be legally competent. The company is responsible for ensuring that all users satisfy these requirements. The managing director, authorised signatory, persons authorised to oblige the company and access control manager are responsible for maintaining the access rights of online banking users. If the company deems it necessary to revoke user access to online banking, the access control manager can suspend access or request that the Bank do so.

3.2.1 Data portal external to online banking

The company can apply for access to a B2B data portal linking the company and the Bank. B2B is an add-on to corporate online banking that enables data sharing between the Bank and a company's accounting software. Once the Bank has approved a B2B application, the company agrees to take every security precautions concerning users authorised by the company to use this connection. Furthermore, the company is fully aware that access control is completely its responsibility. An service provider internal or external to the company handles instalment of B2B. Instalment is not the Bank's responsibility. The company shall be responsible for all actions carried out by its employees using the B2B connection. Furthermore, the company shall be responsible for any measures it considers necessary to ensure the security of its banking information and the legality of the processing of all personal data, and the traceability of entries carried out through the B2B connection. The company shall be liable for any damages suffered by the Bank or a third party as a result of use of the B2B connection by the company and its employees. The same applies to external parties who gain information about access to the system or access it in another manner. The Bank shall not be liable for any damage resulting from the incorrect functioning of equipment to be provided by the

company or software house. The Bank shall not be liable for any damage suffered by the company due to the company's employees' misuse of their authorisations to carry out actions using the B2B connection. In concluding this Agreement, the company authorises the Bank to obtain information on the company's accounts payable from RB for use by other parties utilising a BTB connection. The Bank is not responsible for ensuring that information sent via B2B is accurate, reliable or new. Access to B2B may be terminated by either party with one month's notice.

4 Bank accounts

4.1 About bank accounts

A bank account is created in the customer's name (here after "the Account Holder"). An account used to carry out payments may be a payment account, cf. the Act on Payment Services. The Bank uses different terms to denote different account types and whether an account is a payment account depends on the type. In addition to these Terms, individual accounts may be subject to other of the Bank's special terms and conditions and rules. The terms and conditions for accounts are published to and accessible on the Bank's website. The customer creates an account using self-service solutions or in a Bank branch. The Bank is authorised to reject new accounts, for instance if information about the customer is insufficient, and will notify of such rejection as promptly as possible. Accounts may not be established on behalf of another party unless the customer has granted power of attorney to the effect, unless otherwise provided for by law. Upon establishing an account, the customer is obliged to provide proof of identity by showing valid identification, such as a passport, Icelandic identity card, driver's licence, valid electronic ID, through verification/authentication upon logging in to online banking or other means of identification that meat with the Bank's requirements at each time. The Bank reserves the right to amend its security requirements without notice.

Accounts are in Icelandic króna (ISK), unless otherwise expressly agreed. These Terms apply to accounts both in foreign currency and in ISK, having regard for the special provisions these Terms contain for accounts and payments in foreign currency.

As regards the balance on bank accounts, special terms and conditions apply to each account type. The terms and conditions of an account may provide for a fixed term of deposit and conditions that apply to withdrawal once the fixed term elapses. The rules of the Central Bank of Iceland on the Price Indexation of Savings and Loans at each time apply to inflation-indexed accounts, in addition to the terms and conditions of the account in question.

4.2 Security numbers and access to accounts

The customer chooses a security number to use for authentication and confirmation of payments in communication with the Bank, for example, through online banking, telephone banking and with the Customer Service Centre. In selecting a security number, the customer shall take care not to select a number that can easily be traced back to the customer. The customer agrees not to divulge the security number to unauthorised parties. Unauthorised parties here refers to parties who are not authorised to issue payment orders for the customer's account in accordance with these Terms. Should the customer have reason to believe that an unauthorised party may have become aware of the security number, the customer agrees to change the security number immediately and notify Landsbankinn without delay. The customer is responsible for all payments and actions carried out using his/her security number or other personalised security credentials.

4.3 Payment orders and payment execution

An account can be linked to the payment instrument provided by the Bank. A payment instrument in these Terms refers to any personalised equipment and/or method the Bank and customer agree upon and the customer utilises to issue payment orders, such as payment cards or electronic/digital means of payment. The terms and conditions of the relevant payment instrument further apply to its use.

When the customer issues payment orders, they shall verify their identity or provide other adequate means of authentication that satisfy the Bank's requirements. The above applies whether or not the withdrawal is carried out by using payment instrument or not.

Time of reception of payment orders is the time such orders are received by the Bank. For certain payment types, the Bank may specify closing hours on a banking day as a reception deadline and any payment orders received after the deadline will be considered received on the following banking day. The Bank shall not be considered to have received payment instructions until the Bank has received all information necessary to carry out payment. When the Bank has received payment orders denominated in Icelandic króna, the payment is credited to the account of the payment service provider of the recipient no later than at the end of the following banking day. Domestic payments in Icelandic króna are performed during the opening hours of the interbank system of the Central Bank of Iceland, as listed on its website. When the Bank has received payment orders denominated in euros, the payment is credited to the account of the payment service provider of the recipient no later than at the end of the following banking day, provided payment is carried out within the European Economic Area and meets SEPA requirements. Otherwise, payment orders in a foreign currency are credited to the account of the payment service provider of the recipient five banking day following reception, provided no special circumstances lead to delay.

The Bank may delay, halt and/or refuse to carry out payment orders, initiated by either payor or recipient, if the conditions of law, these Terms, other terms and conditions or the Bank's rules have not been met, e.g. of the balance on the account is insufficient, if withdrawals have been suspended for other reasons, for security reasons, if there is considered to be a risk of misuse or fraud, due to significantly heightened risk of the payor being able to make payment, if there is doubt concerning the payor's authority to utilise the account or for regular monitoring of payments that involves gathering information about the connection between payor and recipient, origin of funds, purpose of a transaction, etc. The Bank uses foreign intermediaries to send and receive international payments on behalf of

customers. For that reason, the Bank may request details about payments and share that information with foreign intermediaries.

The customer will be notified of Landsbankinn's decision to reject payment orders, unless otherwise indicated by law. If the customer is the cause of the Bank's decision to reject payment orders, a fee may be charged for written notification. If payment orders are rejected by the Bank, this is equivalent to such orders not having been received at all. Notwithstanding the above, the Bank may postpone carrying out payment orders until sufficient funds are available on the customer's account, including funds to cover fees and other expenses. The Bank may attempt to debit the payment from the customer's account to satisfy payment following reception of payment orders and until the orders have been carried out. If Landsbankinn receives multiple payment orders the same day, the Bank is not responsible for the order in which the instructions are carried out or which payments are not carried out due to insufficient account balance.

A priori received payment orders will be carried out despite latterly occurring events that would have prevented their issuance, such as the revocation of power of attorney or death of the customer. The customer may only recall or halt payment orders if the relevant provisions of the Act on Payment Services have been met and provided the customer is a consumer. The Bank may demand a fee for recalled payment orders. A priori received payment orders will as a rule not be carried out after the termination of an account. The Bank is responsible for the payment being carried out in accordance with law until the recipient bank has received the payment. After that time, the recipient bank is responsible for the handling of the payment. The customer is responsible for ensuring the accuracy of payment instructions. The Bank is not responsible for the customer's mistakes, inter alia, the customer entering erroneous identification for the recipient. Such mistakes cannot be corrected unilaterally by the Bank without the approval of the recipient of the payment. If a customer can provide evidence to show that the amount of a payment, authorised by the customer and initiated by the recipient, was not specified in the issued authorisation and that the customer's account was debited for a higher amount than he/she could reasonably expect based on his/her spending patterns, these Terms and other circumstances of the case, the customer shall notify the Bank and request repayment within eight weeks of funds being debited from his/her account. These conditions being met, the Bank shall refund the customer such payments within 10 banking days of receiving notice to the effect from the customer. Otherwise the Bank will refuse repayment. The above does not apply when a customer, who is not a consumer as defined by the Act on Payment Services as subsequently amended, orally consents to a third party withdrawing funds from his/her account. The customer is not entitled to repayment once they have directly authorised the Bank to carry out payment and, if appropriate, the Bank or the recipient provided a priori information about payments or transmitted such information to the payor at least four weeks prior to the date of payment. If payment orders have been revoked, Landsbankinn is neither responsible for paying interest nor other fees levied on overdue payments.

Payment services are subject to limitations that may be provided for by foreign currency laws at each time, rules set to enforce such laws and regulations about required information with the transfer of funds. If regular payments have been agreed upon, the notice of termination shall factor in collection of payments following termination of a contract. The Bank is authorised to charge a fee on transfers from the payment account. The Bank may also charge a fee for assistance granted in recovering mistakenly paid funds, e.g. due to erroneous information about the recipient of payment issued along with instructions for payment. Fees are in accordance with the Bank’s tariff of charges at each time.

If a user of Landsbankinn’s payment services is not a consumer, the provisions of Chapter IV and the provisions of the first and second and paragraphs of Article 62, the third paragraph of Article 64, Articles 78, 80, 82, 83, 86 and 93 of Act No. 114/2021, on Payment Services, do not apply to the services.

4.4 Information about an account and its use

Messages, information and notices about accounts, such as about changes to terms and conditions, interest rates and costs, and a statement of fees according to the Act on Payment Accounts, are communicated to customers via the Bank’s website or in online banking or the app or another manner chosen by the Bank. The Bank may also use mail in exceptional cases. The fee for mailing service is listed in the tariff.

4.5 Accounts and payments in foreign currency and reference rate

Payments between accounts in different currencies constitute foreign exchange trading. The Bank bases FX transaction calculations on a reference rate, the general exchange rate. The Bank publishes information about the general exchange rate on its website. The Bank bases purchase and sale of notes in ATMs and branches on a reference rate, the note rate. The Bank may also employ special exchange rates as reference rates in certain types of transactions. Special rates are published in relation to the relevant transactions. Exchange rate changes are based on buy/sell offers on the FX interbank market or on the exchange rate change of foreign currencies, plus a premium. The Bank also uses a reference rate to convert amounts from overseas payment card transactions into ISK and publishes information on this practice on its website. The exchange rate to convert foreign payment card transactions and transactions in a currency other than the base currency of a payment card vary based on changes to the exchange rate quoted by the relevant payment card company plus a premium or, as the case may be, discounts. Changes to exchange rates that are based on changes to a reference rate in accordance with these Terms become effective immediately and without notice. The customer enjoys currency gains or suffers currency loss based on the exchange rate developments of the currencies in question.

Foreign currency accounts and payments are subject to the Act on Foreign Currency and the foreign exchange rules based on the Act. The customer is responsible for ensuring that all data and information, in any form, that the customer provides the Bank with in relation to foreign currency trading or cross-border capital movement is accurate, authentic and reliable.

4.6 Interest and interest rate calculation for bank accounts

Interest rates for accounts vary unless otherwise expressly agree and are in accordance with the Bank's interest rate tariff for each account type. The interest rate tariff is published to an available on the Bank's website. Changes to the interest rate tariff are announced on the Bank's website, through online banking, the app or in another manner chosen by the Bank. Interest rate decisions are based, among other considerations, on the rates of the Central Bank of Iceland, market rates and other funding terms of Landsbankinn. Changes to deposit rates of payment accounts enter into effect two months following notification. Special terms and conditions of accounts may provide that interest rate changes are based on reference rates or reference price and such changes shall enter into effect immediately and without notice upon changes to the Bank's interest rate tariff. The same applies to interest rate changes the Bank deems beneficial to the customer. Notwithstanding the above, all interest rate changes to accounts of customers other than consumers as defined in the Act on Payment Services become effective immediately upon changes to the interest rate tariff.

Deposits carry deposit rates as of the date of deposit and to the date of withdrawal unless otherwise expressly agreed. The last day included in interest calculations is the date prior to withdrawal. Interest is generally added to the balance at the end of each year or when an account is closed. In the case of fixed-term accounts, interest added to the balance at the end of year may be restricted in the same manner as other deposits. As a general rule, interest is calculated for 360 days per annum (the interest year). Each month carries an interest term of 30 days. The beginning of each term depends on the account type and the current terms and conditions for each account. For inflation-indexed accounts, indexation is calculated at the end of each month based on the Consumer Price Index for indexation and is in general added to the principal at the end of each month. Financial income tax is levied on paid interest, indexation and currency gains in accordance with law and debited from the account.

4.7 Overdraft and non-sufficient funds withdrawals

The customer is obliged to monitor the balance on his/her account and may not withdraw from the account an amount that is in excess of its balance or authorised overdraft. If the customer overdraws their account or exceeds the approved overdraft authorisation (e.g. with a non-sufficient funds (NSF) debit card transaction) or the overdraft authorisation is cancelled on other grounds, the customer shall pay a fee for NSF withdrawals according to Landsbankinn's tariff. The fee for the above is charged on each NSF withdrawal. Unapproved overdraft becomes due on the day it is created and bears penalty interest from the transaction date (i.e. the day the payment is registered in Landsbankinn's systems) and to the date of payment. If a customer deposits funds to his/her account after having made NSF withdrawals or exceeded overdraft authorisations, the Bank reserves the right to first utilise those funds to pay the cost of unauthorised overdraft, including collection and legal fees, then to discharge penalty interest, and finally to discharge excess overdraft payments. In the event of failure to rectify default, the Bank reserves the right to foreclose the debt, without notice and with immediate effect, and to enforce the claim through collection. The Bank is authorised to entrust collection to of the claim to a third party. Fees for primary and interim collection are in accordance with the Bank's current tariff or the tariff of the external collector and fees for legal collection are in accordance with the tariff of the relevant collection agent.

4.8 Account transactions and statements

An overview of all transactions on accounts (account statements) are accessible through online banking. Annual statements are published electronically to online banking. A customer who does not have access to online banking can request to have annual statements mailed. The customer shall regularly review his/her account statements. The customer shall notify the Bank without undue delay should they notice unauthorised or wrongful payments which that give rise to a claim for correction (see Section 6).

Landsbankinn refunds amounts which the Bank verifiably wrongly withdraws from its customers' accounts.

The customer authorises the Bank to reverse and/or correct amounts erroneously or due to a system error deposited to an account. Such corrections shall take place without undue delay and appear on the customer's account statements.

The customer shall review all information prior to making payment to a third party account, regardless of whether such payment is made with a payment instrument, through online banking, via telephone, with a teller or using other means. The customer is responsible for ensuring the accuracy of information about amount, recipient and any accompanying messages.

4.9 Closing of bank accounts and other services

A customer wishing to close an account may submit a written request to the Bank, request it verbally over the phone or, as the case may be, close the account independently in self service. Should the customer terminate these Terms, the Bank reserves the right to terminate accounts and other services, including online banking, in part or in full, temporarily or permanently, at its own initiative and without first notifying the customer. The same applies if a customer is demonstrated to have committed an offence against law, the Bank's rules, its terms and conditions or other rules applying to the customer's business with the Bank, if the customer or a third party is demonstrated to have misused an account, the customer fails to comply with the Bank's request to update or submit information during regular monitoring of money laundering and/or terrorist financing, if transactions are considered by the Bank to constitute a risk of fraud, money laundering and terrorist financing or if the business relationship might damage the Bank's reputation or does not conform to the Bank's risk policy, in its estimation. In such cases, the Bank may deposit the balance of accounts to an account held by the Bank. The Bank further reserves the right to close an account that has been inactive for a period of 2 years or longer, following a notice to the effect to the customer, and deposit the balance to another account held by the customer or, if the customer does not own a second account, to an account held by the Bank. Any fees or costs owed the Bank by the customer for services rendered when an account is closed in

accordance with the above, may be debited from the customer's account prior to its closing. In the case of any negative balance on the customer's account upon closing, e.g. charged fees, the Bank reserves the right to enforce the claim through collection. The customer will be notified of the closing of the account as promptly as possible.

5 Payment cards

5.1 About payment cards

Payment cards refers to debit and credit cards (hereafter referred to jointly as "payment cards" or "cards"). A payment card is linked to a specific payment account for debit cards or card account for credit cards (in Section 5, payment accounts and card accounts will be referred to jointly as an "account"). Cards can be used to pay for goods and services, to withdraw funds or other purposes which accord with the provisions of these Terms and other rules on payment card use that may be valid at each time. The account holder may request the issue of multiple debit cards to his/her payment account. If the account holder requests that the Bank issue a card linked to his/her account to a third party, the account holder authorises that party to oblige the account holder and utilise the card in accordance with these Terms. Payments/withdrawals using a card are debited from a payment account or registered to a card account. The account holder pays the cost of issuance and use of a card in accordance with the Bank's price tariffs. The account holder also pays the cost of using a card charged by other service providers, including fees that ATM service providers charge on withdrawals. The card holder is the person to whom a card is issued. The card holder may be the account holder or a person authorised by the account owner to carry a card linked to the account. The card holder is also an individual who holds a company card. Retail payment cards are issued to individuals. Corporate payment cards are issued to individuals who are sole proprietors or to the registration numbers of legal entities, such as associations, companies and institutions. The legal entity is the account holder and is responsible for all use, payments and withdrawals made by the card holder. The international terms and conditions of the relevant payment card scheme (e.g. VISA or MasterCard) also apply to payment cards and are published on their websites.

5.2 Application and issuance

A payment card is issued by the Bank and is its property. The account holder applies for cards in a branch, via telephone or electronically, e.g. Through online banking or the app. The Bank reserves the right to reject card applications. A card is issued to the card holder's name. The card holder uses personalised security credentials, such as a security number/PIN to confirm payment/withdrawal. The Bank determines the validity period of the card and registers it on the back of the card. The card is valid until the last day of the month specified on the card. A card holder or account holder who does not wish to renew a card shall notify the Bank in writing no later than one month prior to the end of the validity period. When a card is issued and renewed, a new card is sent to the card holder's legal domicile or registered address. Corporate cards are sent to the legal domicile of the account holder. The account holder can request that a card be sent to a Bank outlet or branch. The fee for issuance and renewal is in accordance with the Bank's tariff. If the card holder does not receive the card within a reasonable time frame, they shall notify the Bank without delay.

5.3 Use of payment cards

The Bank unilaterally determines maximum withdrawal amounts for cards, such as in ATMs and POS card readers, and reserves the right to refuse to raise the limit. The card holder agrees not to exceed account limits in his/her use of the card. Otherwise charges may apply based on the tariff, and criminal liability based on law. If there are reasoned grounds to suspect unauthorised or fraudulent use of a card or if the use of a card contravenes these Terms, the Bank reserves the right to reject withdrawals and close a card and demand that it be returned to the Bank. The Bank reserves the right to amend its security requirements without notice.

Verification/authentication is a method that allows the Bank to verify the customer's identity or confirm authority to use a specific payment instrument, including the use of personalised security credentials. Authentication involves entering personalised security credentials such as a PIN or unique identifier number/code, other security number for authentication purposes or use of biometrics. Authentication may also involve other methods, depending on the Bank's security requirements at any given time. The Bank determines the requirements for verification/authentication.

Recurring payment orders are based on an agreement between the merchant (payment recipient) and card holder, whereby the card holder agrees that regular payments for goods and services are debited to a payment card, and constitute a priori payment orders. If a card is cancelled or renewed with a new number, the Bank is authorised to debit recurring payment orders to the new card or another payment card owned by the card holder. The Bank shall not be responsible for damage or loss the card holder may suffer if payment orders are not executed. Should the card holder wish to recall or cancel recurring payment orders, they should contact the merchant.

5.4 Obligations and safekeeping

The card holder is responsible for safeguarding the card, PIN, unique identifier numbers/codes and other personalised security credentials to prevent third parties from gaining access to the card, personalised security credentials or other information about the card, such as the card number or security number. The card holder may not deliver the card, PIN, unique identifier numbers/codes or other personalised security credentials or other information about the card to a third party and the card holder shall at all times ensure the security of the information. The card holder may not store the PIN or other personalised security credentials with the card, in his/her wallet, mobile phone, online or in other electronic media or in another manner that may be accessible by a third party. The card holder may not copy the card or alter its functionality. The card holder shall show enhanced precaution as regards false messages, such as text messages or emails, which the card holder may receive from a third party, for such purposes as gaining access to personalised security credentials or other information about the card. Failure by the card holder to adequately safeguard the card, PIN, other personalised security credentials or other information about the card or in accordance

with the above is considered gross negligence. The card holder should at all times ensure that no one can view the PIN, other personalised security credentials or other information about the card. The card holder shall not authorise the execution of a payment with a unique identifier number/code they may have received, unless they have ensured that the amount, currency and recipient are correct. Failure by the card holder to uphold precautionary obligations in accordance with the above is considered gross negligence on behalf of the card holder.

The card holder or account holder cannot recall payments/withdrawals the card holder performs with a card or token linked to it. The card holder is responsible for payments/withdrawals his/she has confirmed by signing a sales receipt or entering personalised security credentials (e.g. a PIN), by entering card information in the appropriate fields when purchasing goods or services on the Internet or divulging such information verbally, by divulging information about the security number via telephone payment, by a priori authorisation to merchants, by carrying out contactless payment, by confirming payment using a unique identifier number/code or by approving the implementation of payment/withdrawal in another manner that accords with the Bank's rules at each time. The card holder shall his-/herself carry out payment/withdrawal and enter the PIN or other personalised security credentials or information about the card. Failure by the card holder to safeguard the card, PIN or other personalised security credentials or other information about the card in accordance with these Terms, results in liability for all payments/withdrawals carried out with the card. The Bank assumes that all payments/withdrawals with the card are carried out by the card holder and in accordance with the account holder's wishes. If the card holder is not also the account holder, the account holder and card holder bear full responsibility for usage of the card an all payments/withdrawals made with the card. Payments/withdrawals with the card are entered on the transaction statement of a card account/account statement for payment accounts ("statement"). The statement contains information about the itemised amounts of payments/withdrawals, exchange rates, amount of payment following currency conversion, validity date of debit entries or date of reception of payment instructions, name of merchant and information about payments payable on the next due date for payment. Statements are otherwise subject to these Terms as appropriate.

The provisions of Chapter 6 of these Terms apply to liability for payment cards. If the card holder or account holder consider themselves to have suffered damages, they shall notify the Bank in a verifiable manner. If the conditions of the chargeback rules of the international card schemes (e.g. VISA or MasterCard) are satisfied, the card holder or account holder shall lodge a chargeback claim based on those rules in a format supplied by the Bank. The Bank acts as intermediary for the chargeback claim which is processed by the international card schemes. The rules of the card schemes are accessible on their websites. The Bank shall have no connection with, or bear any responsibility for, any dispute or loss resulting from the purchase of goods or services paid for with the card. The Bank shall not be liable for damages incurred by the card holder or account holder due to technical failure in ATMs or other equipment nor for damages suffered by the card holder or account holder if equipment fails to contact the Bank's authorisation system.

5.5 Lost cards, closing and cancellation

If a card is lost or the card holder thinks that his/her card has been used without authorisation or misused, he/she or the account holder shall notify the Bank without delay during office hours or by calling the emergency hotline of the relevant card company outside office hours. Immediately following such notification, the card and/or token is closed, temporarily or permanently, or it recalled, to prevent further use or misuse thereof. The card holder is obligated to assist the payment card company and the Bank in such matters and seek to minimise losses in so far as possible. The Bank may require the card holder to submit a written declaration stating that a card has been lost and a written request for a new card. If a card holder loses his/her card while overseas, he/she can get emergency cash through the intermediation of a payment card company. The cost of this service as provided for in the current tariff will be debited from the account holder's account. If a card holder subsequently finds a card which has been reported as lost, he/she may not use this card, unless with the Bank's permission. The Bank must be notified that the card has been found and it returned to the Bank. If the card holder wishes to reopen the card, he/she shall be responsible for all use of the card during the period it was lost. A request for the reopening of a card shall be made in writing or confirmed in a verifiable manner.

The card holder and account holder may close a card at any time. If the card holder wishes to terminate a card or rescind their application, they shall notify the Bank. The Bank may, without prior warning or notice, refuse to carry out payment orders or withdrawals, close or limit the card holder's access to a card, temporarily or permanently, or recall it without prior notice if (a) a card has been reported as stolen or lost, (b) if there is reason to suspect that a third persona has gained access to the card, personalised security credentials or other information about the card, with or without the card holders authorisation, (c) a payment account has either been closed or destroyed, (d) if a card has been closed, (e) if the amount of payment (with added cost, as the case may be) exceeds the account balance or limit or debt owed the Bank foreclosed, (f) wrong personalised security credentials have been used, e.g. a wrong PIN, (g) the validity period of the card has expired, or, (h) if there is reason to suspect that the card holder has violated the rules and terms and conditions that apply to the card, (i) if an account holder, card holder, or guarantor is subjected to distraint; if a request is made for bankruptcy proceedings against these parties; if these parties request composition of creditors; or if other cards issued to these parties are closed, (j) if the Bank is forced to write off unpaid claims on the card holder or account holder or if the account holder and/or card holder defaults, (k) if a card has not been used for a period of 12 continuous months or the annual fee on a card has not been paid; or (l) if the card holder does not have a valid due diligence. The card holder is notified of such closure. If these suspicions prove to be unfounded, the card is re-authorised for use. If a card is recalled, the card holder shall return it the next branch without delay. If the card holder fails to return the card, the Bank can request repossession of the card. A card holder may not use the card after it has expired, has been cancelled or is in some other way unusable.

5.6 Settlement and payment for credit cards

The account holder receives an invoices for credit card use in online banking. If the account holder or card holder have authorised the Bank to debit payments from a payment account, direct debit is undertaken on the due date for

payment of the card invoice. If there are insufficient funds on the customer's payment account on the due date for payment of a credit card bill, the Bank may equalise any existing balance against the owed amount and continue to seek fulfilment until the debt is paid in full. The transaction date determines the allocation of a payment/withdrawal to a withdrawal period. The registration date of a transaction by merchant may lead to a transaction being registered to the following withdrawal period. The general withdrawal period, on which the card holder's transaction statement is based, is a month, with the end and beginning advertised on the Bank's website. If the due date for payment falls on a weekend or bank holiday, the due date for payment shall be the next banking day. If payment has not been remitted by this time, the card holder is liable for the payment of penalty interest from the payment deadline until the date of payment; penalty interest shall be charged at the rate advertised by the Central Bank of Iceland. The card holder can withdraw the positive balance on a card account on the next due date for payment following the withdrawal period during which the positive balance was created. If the card holder is the account holder, he/she can raise/lower the credit card limit in online banking for a fee according to the Bank's tariff. The maximum limit is based on the current credit framework at each time.

If a card has been cancelled or closed, the Bank debits outstanding payments to the card account. In the case of current payment equalisation services upon closure or cancellation, instalments plus interest and costs are debited to a card account. On the due date for payment, the outstanding amount is debited to the card holder's account for debit. Where there is no registered account for debit, the card holder receives an invoice to online banking. The Bank may, yet is not obligated, to transfer the outstanding amount on a card account to a new card issued to replace a closed or cancelled card, or to another card owned by the account holder. The same applies to amounts outstanding payment equalisation services. The account for debit and, as the case may be, any collateral pledged to guarantee repayment on time and without loss in connection with the card will be valid for the new card also or another card owned by the account holder.

6 Liability for payment services

The payor shall notify the Bank without undue delay of any unauthorised or erroneously executed payment. Notification shall be delivered to the Bank no later than 13 months after the date of a debit transaction in the case of consumers and no later than 120 days from the date of a debit transaction in the case of a legal entity. Provided legal provisions of payment service and/or the provisions of these Terms are met, the Bank refunds the payor the amount of the unauthorised payment. The Bank will return the balance of the payment account previously debited to its position before the unauthorised payment took place. The payors failure to notify the Bank without undue delay in accordance with the above may lead to forfeiture of the right to refund. If the payor is suspected of fraud, the Bank may refuse to refund and notify the Financial Supervisory Authority of the Central Bank of its suspicions.

The payor shall bear the loss of unauthorised payments up to the equivalent amount of 50 euros in Icelandic króna based on the public reference rate (mid-rate) as it is listed at each time when the loss can be traced to the use of lost or stolen payment instrument or the unauthorised use of a payment instrument. This shall, however, not apply if: (a) the payor could not have known that the payment method was lost, stolen or being used in an unauthorised manner and the payor has not acted in a fraudulent manner, or (b) the payors loss of the payment instrument is attributable to the action or inaction of the Bank's employee, agent or contractor. Notwithstanding this, the payor shall bear all loss that results from unauthorised payments if the payor has instigated them in a fraudulent manner or failed to perform one or more of his/her obligations under the law or these Terms in connection with the payment instrument and/or personalised security credentials intentionally or through gross negligence. When this is the case, the aforementioned maximum amount does not apply. When the payors actions have been neither fraudulent nor negligent, nor has the payor intentionally failed to fulfil his/her obligations under the law or these Terms in connection with a payment instrument and personalised security credentials, regard shall be had for the nature of the personalised security credentials of the payment instrument and circumstances surrounding loss of the payment instrument, theft thereof or unauthorised use there, in determining the amount the payor's own liability, cf. above. The payor, if he/she is a consumer, shall not suffer the damages caused by use of a payment instrument which is lost, stolen or used in an unauthorised manner following notification of the loss, theft or misuse use of the payment instrument or unauthorised use thereof, provided the payor has not acted fraudulently.

Landsbankinn's liability for payment that does not take place or is faulty shall be as provided for in the Act on Payment Services, provided the payor is a consumer. Landsbankinn is not liable for damages or is otherwise liable for payment services if damages can be traced to unnatural or unforeseeable circumstances which the parties to the case did not affect nor could hinder despite attempts to do so. The same applies to damages under other laws on payment service providers.

Liability for payment services shall in other respects comply with the Act on Payment Services. If a user of Landsbankinn's payment services is not a consumer, the first and second paragraphs of Article 62, the third paragraph of Article 64, Articles 78, 80, 82, 83, 86 and 93 of Act No. 114/2021, on Payment Services, do not apply to the services.

7 Final provisions

Unless otherwise specified by statute, contractual provisions, these Terms, other terms and conditions, the Bank's rules or according to the nature of the matter, the Bank and the customers may end their mutual business relationship at any time without notice. The customer shall notify the Bank in writing of his/her decision to end the business relationship with the Bank or revocation of consent to process personal data. The Bank may terminate a framework agreement with two months' notice, in accordance with these Terms. The Bank reserves the right to end a business relationship, in full or in part, of its own initiative with a unilateral notice to the customer if the customer is demonstrated to have committed an offence against law, the Bank's rules, its terms and conditions or other rules

applying to his/her business with the Bank, if the customer or a third party is demonstrated to have misused the business relationship, if transactions are considered by the Bank to constitute a risk of money laundering or terrorist financing, if the business relationship might damage the Bank's reputation, or does not confirm to the Bank's risk policy, in its estimation. The Bank may terminate a contract for a consumer's general payment account in accordance with legal provisions of the Act on payment accounts.

If communications leading up to and the establishment of this Terms are solely telecommunications, the Terms shall be considered a distance contract as provided for in Act No. 33/2005, on Distance Sales of Financial Services. If the customer is a consumer he/she has the right, having regard for the limitations set out in the Act on Distance Selling of Financial Services, to abandon the Terms if they constitute a distance contract as defined in the aforementioned Act without specifying a reason, provided he/she verifiably notifies the Bank thereof within 14 days of approving the Terms.

The customer may refer any dispute with the Bank to the Complaints Committee of Transactions with Financial Firms (appeal) provided relevant requirements, set forth in the Committee's Articles of Association, are met. The address of the Committee is Guðrúnartún 1, 105 Reykjavík. The Committee's website is https://nefndir.is/fjarmala/. Any disputes over the violation of these terms may be brought before the District Court of Reykjavík. All disputes concerning business with the Bank shall be resolved in accordance with Icelandic law, unless otherwise agreed.

The Bank shall not be responsible for any direct or indirect loss which the Customer may incur in connection with these Terms and Conditions or transactions concluded on their basis if such loss can be attributed to events resulting from force majeure, such as natural catastrophes, wars, terrorist activity, strikes, border closures, electricity disruption or failure, disruption of a settlement system, telephone system or other communication routes, or other similar events. Nor shall Landsbankinn be responsible for any inconvenience, expense, missed investment opportunities or other direct or indirect financial loss resulting from the closure, failure, interruption or other disruption of the Bank's activities.

These Terms are originally published in Icelandic. The Icelandic language version shall be the sole valid version of these Terms, regardless of whether the Bank chooses to publish these Terms in another language. Icelandic law shall apply to these Terms.

These Terms shall apply as of and including 1 August 2023. This notwithstanding, these Terms shall apply as of and including 1 June 2023 for customers who confirm the Terms as of that date.