УТВЕРЖДЕНО:

Правлением

ООО КБ «РостФинанс»

Протокол №23 от «25» марта 2020г.

ВВЕДЕНО:

Председатель Правления

ООО КБ «РостФинанс»

А.Б. Прохватилов

Приказ №163 от «27» марта 2020г.

ПРАВИЛА
дистанционного банковского обслуживания физического лица в Системе «iBank2» в ООО КБ «РостФинанс»

г. Ростов-на-Дону
2020 год

Содержание

1. Термины и определения

1.1.**Авторизационные данные** – логин и самостоятельно созданный Клиентом Пароль.

1.2.**Авторизация –** процедура распознавания Клиента в Системе «iBank2» с целью получения Банком подтверждения возможности предоставления Клиенту услуг дистанционного банковского обслуживания через Интернет.

1.3.**Аутентификация** – подтверждение подлинности передаваемых Клиентом в Банк Электронных документов. Положительный результат Аутентификации подтверждает, что операция производится самим Клиентом. Положительным результатом аутентификации считается совпадение Логина Клиента с соответствующим ему Паролем.

1.4.**Банк** – Общество с ограниченной ответственность коммерческий банк «РостФинанс» (ООО КБ «РостФинанс») и его структурные подразделения.

1.5.**Блокировочное слово**– уникальное слово на русском языке, определяемое Клиентом при регистрации в Системе «iBank2», для блокирования работы и идентификации Клиента по телефонному звонку в Банк.

1.6.**Внутрибанковский перевод –** перевод денежных средств, осуществляемый Банком по распоряжению Клиента о списании денежных средств со своего Счета и их перечисление на счет получателя средств и/или о совершении операций между своими счетами в Банке.

1.7.**Внешний перевод** – перевод денежных средств, осуществляемый Банком по поручению Клиента на счета, при наличии у Банка технической возможности, открытые в другой кредитной организации, по реквизитам, указанным Клиентом.

1.8.**Временные авторизационные данные –** логин и временный пароль.

1.9.**Выгодоприобретатель** – лицо, к выгоде которого действует Клиент при проведении операций с денежными средствами и иным имуществом. **Выгодоприобретатель** – лицо, не являющееся непосредственно участником операции, к выгоде которого действует Клиент, в том числе, на основании агентского договора, договоров поручения, комиссии и доверительного управления, при проведении операций с денежными средствами и иным имуществом;

1.10.**Договор** – договор на обслуживание физического лица в Системе «iBank2», заключаемый между Клиентом и Банком на основании Заявления Клиента в совокупности с Правилами и Тарифами.

1.11.**Заявление** – заявление о присоединении к Правилам дистанционного банковского обслуживания физического лица в Системе «iBank2», содержащее сведения о Клиенте и являющееся неотъемлемой частью Договора на обслуживание физического лица в Системе «iBank2».

1.12.**Клиент** – физическое лицо, заключившее с Банком договор банковского (текущего) счета (вклада).

1.13.**Ключ электронной подписи** – уникальная последовательность символов, предназначенная для создания Электронной подписи.

1.14.**Компрометация информации** - факт доступа постороннего лица к защищаемой информации, а также подозрение на него.

1.15.**Лимит -** максимально допустимая сумма денежных средств для переводов в течение определенного периода (суток и месяца), установленная Банком, по операциям, проводимым Клиентом в Системе.

1.16.**Логин** – уникальная последовательность символов (комбинация букв и/или цифр), присваиваемая Клиенту Банком и позволяющая однозначно идентифицировать Клиента в Системе «iBank2».

1.17.**Мобильное приложение** - специальное программное обеспечение (приложение), которое используется для работы в Системе «iBank2» с использованием мобильного устройства Клиента (мобильный телефон / планшет).

1.18.**Пароль** – самостоятельно созданная Клиентом последовательность символов, удовлетворяющая определенным требованиям, используемая для подтверждения принадлежности Клиенту используемого идентификатора (Номера пользователя) и Учетной записи, позволяющая Клиенту подтвердить свою подлинность в Системе **«iBank2».** При регистрации Клиента в Системе **«iBank2»** Клиенту на мобильный телефон посредством SMS-сообщения направляется временный пароль, который используется для первичного входа в Систему. При первичной авторизации Клиента в Системе **«iBank2»** принудительно запускается режим смены пароля.

1.19.**Признаки осуществления перевода без согласия клиента** – критерии и параметры операций, установленные Банком, при которых у Банка возникает подозрение, что операция является следствием неправомерных действий третьих лиц, а также критерии и параметры операций, установленные Банком России.

1.20.**Подключение Клиента** – процесс (совокупность действий) предоставления Клиенту доступа к Системе «iBank2», включая регистрацию Клиента, предоставление ему определенных полномочий в Системе «iBank2» и наложение определенных ограничений на его действия в Системе «iBank2».

1.21. **Пакет электронных документов** - несколько связанных между собой электронных документов, в.т. информационное письмо свободного формата и вложения к нему.

1.22.**Правила –** Правила дистанционного банковского обслуживания физического лица в Системе «iBank2» ООО КБ «РостФинанс», размещенные на сайте Банка www.rostfinance.ru в сети Интернет.

1.23.**Простая электронная подпись** – Электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования Электронной подписи определенным лицом.

1.24. **Разовый пароль** – направленный Банком посредством SMS-сообщения на мобильный телефон Клиента, указанный в Заявлении, случайный, уникальный набор символов, используемый Клиентом для подтверждения Электронного документа, переданного через Систему **«iBank2».** Для подтверждения каждого конкретного Электронного документа Системой высылается отдельный разовый пароль. Разовый пароль является текущим в данный момент времени и может быть использован только один раз для подтверждения той операции, для которой он сформирован.

1.25.**Регистрация Клиента** – процесс (совокупность действий) создания Учетной записи Клиента в Системе «iBank2».

1.26.**Система «iBank2», Система** – автоматизированная система дистанционного банковского обслуживания физических лиц, обеспечивающая выполнение обязательств Банка перед Клиентом в рамках заключенного Договора.

1.27.**Средства электронной подписи** – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание Электронной подписи, проверка Электронной подписи, создание Ключа электронной подписи и Ключа проверки электронной подписи.

1.28.**Средства создания электронной подписи –** средства, используемые для создания Электронной подписи, в том числе, Средства электронной подписи (криптографические).

1.29.**Стороны** – Банк и Клиент.

1.30.**Счет** – банковский (текущий, счет по вкладу, счет банковской карты) счет, открытый Клиенту Банком на основании заключенного между Банком и Клиентом в соответствии с требованиями законодательства Российской Федерации соответствующего договора банковского счета.

1.31.**Тарифы –** утвержденные уполномоченным органом Банка Тарифы комиссионного вознаграждения ООО КБ «РостФинанс» по обслуживанию физических лиц.

1.32.**Учетная запись Клиента** – совокупность данных определенного формата в Системе «iBank2», однозначно отождествленных с Клиентом и представляющих его в Системе.

1.33.**SMS-сообщение** (SMS — аббревиатура от английских слов Short Message Service) — сообщение текстового формата, направляемое Банком Клиенту на номер телефона Клиента.

1.34.**Push-сообщение** – всплывающее текстовое сообщение, которое отображается на экране мобильного устройства.

1.35.**SMS/PUSH-уведомление –** форма документированного уведомления в виде текста SMS/PUSH сообщения, направляемого Банком Пользователю на номер мобильного телефона, информация о котором была предоставлена Пользователем в Банк в соответствии с пунктом 9.1 настоящих Правил, по каждой совершенной по банковскому счету/счету по вкладу расходной операции с использованием системы, или для информирования Пользователя о приостановке/отказе от исполнения Банком Электронного документа в соответствии с условиями настоящих Правил .

1.36.**Электронная подпись** – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом

связана с такой информацией, и которая используется для определения лица, подписывающего информацию.

1.37.**Электронный документ** – совокупность данных в электронной форме, подписанная Электронной подписью. Клиент признает, что ЭД, сформированный и переданный в соответствии с настоящими Правилами, имеет равную юридическую силу и влечет такие же правовые последствия, что и документ, оформленный на бумажном носителе и подписанный собственноручной подписью.

1.38.**Электронные устройства (ЭУ)** – устройства Клиента, используемые в качестве удаленного рабочего места для целей дистанционного управления денежными средствами Клиента: персональный компьютер, ноутбук и т.д.

1.39.**SSL соединение** – защищенное сетевое соединение, устанавливаемое по протоколу SSL средствами операционной системы.

2. Общие положения

2.1.Настоящие Правила устанавливают порядок дистанционного банковского обслуживания физического лица в Системе «iBank2» и определяют права, обязанности и ответственность Сторон, возникающие в этой связи.

2.2.Заключение Договора осуществляется Клиентом в соответствии со статьей 428 Гражданского кодекса Российской Федерации путем:

2.2.1. предоставления в Банк двух экземпляров Заявления о присоединении к Правилам предоставления дистанционного банковского обслуживания для физических лиц в Системе «iBank2» оформленного по форме Приложения 1 к настоящим Правилам. Договор между Банком и Клиентом считается заключенным с даты подписания уполномоченным сотрудником Банка Заявления Клиента. Один экземпляр Заявления передается Клиенту, а второй остается в Банке. Заявление, подписанное Клиентом и Банком, является документом, подтверждающим факт заключения договора между Клиентом и Банком.

2.2.2.указания в «Заявлении на получение личных международных банковских карт MasterCard ООО КБ «РостФинанс» и открытие специального карточного счета (СКС)» необходимости предоставления доступа к Системе «iBank2»

2.3.Договор заключается только при наличии у Клиента, открытого в Банке текущего Счета/ текущего счета с использованием международных пластиковых карт.

2.4.Подпись Клиента в Заявлении свидетельствует о том, что он ознакомлен и согласен с Правилами и Тарифами, присоединяется к ним и обязуется их соблюдать.

2.5.Клиент уведомлен об условиях использования Системы «iBank2» в частности о любых ограничениях способов и мест использования, случаях повышенного риска использования Системы «iBank2».

2.6.Банк с целью ознакомления Клиентов с условиями Правил и Тарифов размещает Правила и Тарифы путем опубликования информации одним или несколькими из нижеперечисленных способов:

- размещение такой информации на Сайте Банка в сети Интернет www.rostfinance.ru;
- оповещение Клиентов через Систему «iBank2»;
- размещение объявлений на информационных стендах в подразделениях Банка, осуществляющих обслуживание Клиентов;
- иные способы, позволяющие Клиенту получить информацию и установить, что она исходит от Банка.

Моментом ознакомления Клиента с опубликованной информацией считается момент, с которого информация доступна для Клиентов.

2.7.Настоящие Правила распространяются на все правоотношения с Клиентом, возникшие до введения в действие настоящих Правил, касающиеся дистанционного банковского обслуживания физического лица в Системе «iBank2».

3. Обеспечение безопасной работы в Системе «iBank2»

3.1.Каналы связи общего пользования, используемые для доступа к Системе и передачи Электронных документов, не являются защищенной средой, в связи с чем Клиент принимает риски, связанные с возможным нарушением конфиденциальности, целостности и доступности обрабатываемой информации, в том числе, обусловленным компрометацией Авторизационных данных и Ключей электронной подписи.

3.2.В целях защиты обрабатываемой в рамках Договора информации Банком и Клиентом по взаимному соглашению применяется комплекс организационно-технических мер:

- использование защищенного SSL соединения для обеспечения конфиденциальности и целостности Электронных документов, Авторизационных данных при их передаче по каналам связи общего пользования между компонентами доступа Клиента и Системой «iBank2»;
- использование Электронной подписи, предусмотренной настоящими Правилами, для подтверждения авторства и обеспечения юридической значимости Электронного документа.

3.3.При передаче Электронного документа, Авторизационных данных по защищенному SSL соединению, установленному непосредственно (без промежуточных узлов) между компонентами доступа Клиента и Системой «iBank2», их подделка или иное искажение, а также ознакомление с данной информацией третьих лиц практически невозможно.

3.4. Электронный документ, сформированный и подписанный Электронной подписью средствами Системы «iBank2», равнозначен документу на бумажном носителе, составленному Клиентом и подписанному собственноручной подписью Клиента, если проверка Электронной подписи, проведенная в установленном настоящими Правилами порядке, дала положительный результат и подтвердила, что Электронная подпись сформирована с использованием Ключа электронной подписи Клиента.

3.5.Формирование подложного Электронного документа, равно как искажение сформированного Электронного документа, а также формирование корректной Электронной подписи под подложным Электронным документом практически невозможно за исключением следующих ситуаций:

- Ключ электронной подписи Клиента скомпрометирован;
- Авторизационные данные Клиента скомпрометированы;
- Третьими лицами получен доступ к Авторизационным данным, Средствам создания электронной подписи или связанным с ними компонентам информационной системы Клиента;
- Третьими лицами получен доступ к SIM-карте с номером мобильного телефона, указанного Клиентом в Заявлении, который используется для получения кодов, паролей;
- Защищенное SSL соединение установлено с использованием промежуточных узлов, доступом к которым обладают третьи лица.

3.6.В качестве единой шкалы времени при работе с Системой «iBank2» является Московское поясное время. Контрольным является время системных часов аппаратных средств Банка.

4. Порядок подключения к Системе «iBank2»

4.1.Подключение Клиента к Системе производится на основании собственноручно подписанного Клиентом Заявления, согласно п.2.2.настоящих Правил не позднее рабочего дня, следующего за днем подачи Заявления в Банк.

4.2.Подключение к Системе «iBank2» происходит в полнофункциональном режиме.

Система «iBank2» в полнофункциональном режиме позволяет осуществлять обмен электронными документами при совершении следующих операций:

- переводов в валюте Российской Федерации;
- получения выписки по счетам/ картам;
- переводов в иностранной валюте (при наличии технической возможности);
- отправки сообщений свободного формата в виде электронного письма.

4.3.Подключение Клиенту дополнительных услуг Системы осуществляется Банком на основании соответствующего заявления Клиента установленной Банком формы (включая формы, внедренные в Системе), не позднее следующего рабочего дня после передачи заявления в Банк и оплаты всех причитающихся Банку комиссий в соответствии с Тарифами.

5. Порядок Регистрации Клиента в Системе «iBank2»

5.1.Регистрация Клиента в Системе производится на основании собственноручно подписанного Заявления Клиента, согласно п.2.2.настоящих Правил.

5.2.Банком предоставляются Клиенту Временные авторизационные данные для первого входа в Систему. Логин и временный пароль для входа отправляется в виде SMS-сообщения на указанный в Заявлении номер телефона Клиента.

5.3.Для завершения процесса регистрации Клиент должен осуществить вход в Систему в течение 3 (трех) дней с момента получения SMS-сообщения с Временными авторизационными данными и задать долговременный пароль для входа в Систему.

5.4.После задания Клиентом пароля, удовлетворяющего требованиям безопасности Системы, процесс Регистрации Клиента считается завершенным.

5.5.После завершения процесса регистрации доступ к Системе осуществляется с использованием логина, переданного Банком, долговременного пароля, заданного Клиентом самостоятельно и разовых паролей, передаваемых клиенту с помощью SMS-сообщений на номер, указанный в Заявлении.

6. Порядок использования Простой электронной подписи

6.1.При осуществлении переводов (платежей) на сумму, ограниченную максимальным порогом в день/месяц, определенным лимитом, переводов по своим счетам, а также подключения/отключения услуг банка и партнеров, предложенные в Системе, используется Простая электронная подпись.

6.2.В качестве методов формирования и проверки Электронной подписи используются методы, реализованные в Системе «iBank2» и основанные на применении разовых паролей, выступающих в качестве одноразовых Ключей электронной подписи и одноразовых Ключей проверки электронной подписи.

6.3.Для формирования Электронной подписи под каждым отдельным Электронным документом Клиент использует отдельный разовый пароль, выступающий в качестве одноразового Ключа электронной подписи.

6.4. Разовый пароль, выступающий в качестве одноразового Ключа электронной подписи, Клиент получает в отправляемом Банком SMS-сообщении на телефонный номер, указанный в Заявлении.

6.5.Электронная подпись признается подлинной в том и только том случае, если предоставленный Системе «iBank2» для ее формирования одноразовый Ключ электронной подписи эквивалентен (полностью совпадает) Ключу проверки электронной подписи, сгенерированному Системой.

7. Порядок выполнения операций по счетам

7.1.В Системе «iBank2» Банк предоставляет доступ к текущим счетам Клиента, текущим счетам Клиента с использованием международных пластиковых карт, счетам по вкладам (депозитам), кредитам, а также другим услугам Банка и партнеров банка.

7.2.Все операции осуществляются в пределах остатка денежных средств на счете Клиента с одновременным соблюдением Лимита на сумму проводимых операций. Ограничение на осуществление операций по счетам клиентов указаны в Приложении №12 к настоящим Правилам.

7.3.Все операции по счетам в Системе «iBank2» осуществляются на основании Электронного документа, составленного Клиентом по форме, установленной Банком (включая документы, отличные по форме, но аналогичные по содержанию, утвержденным в Банке) и в порядке, предусмотренном настоящими Правилами.

7.4.Работа со счетами в Системе «iBank2» возможна в следующих режимах:

- Просмотра;
- Пополнения;
- Списания;
- Всех операций.

Режим просмотра в Системе «iBank2» позволяет:

- Просматривать список всех своих счетов/услуг, подключенных к Системе «iBank2», с информацией о текущем остатке денежных средств на них, а также формировать отчет о движении денежных средств по этим счетам за выбранный период (текущим счетам, текущим счетам с использованием банковских карт, депозитным счетам, кредитам и другим услугам, подключенным клиенту.

Режим пополнения позволяет:

- Пополнять денежными средствами текущие счета, а также депозитные счета, если это предусмотрено условиями договора вклада;
- Просматривать список всех своих счетов/услуг, подключенных к Системе «iBank2», с информацией о текущем остатке денежных средств на них, а также формировать отчет о движении денежных средств по этим счетам за выбранный период (текущим счетам, текущим счетам с использованием банковских карт, депозитным счетам, кредитам и другим услугам, подключенным клиенту.

Режим списания позволяет:

- Списывать денежные средства с текущих счетов;
- Просматривать список всех своих счетов/услуг, подключенных к Системе «iBank2», с информацией о текущем остатке денежных средств на них, а также формировать отчет о движении денежных средств по этим счетам за выбранный период (текущим счетам, текущим счетам с использованием банковских карт, депозитным счетам, кредитам и другим услугам, подключенным клиенту.

Режим всех операций позволяет:

- Управлять средствами текущих и депозитных счетов без ограничений;
- Просматривать список всех своих счетов/услуг, подключенных к Системе «iBank2», с информацией о текущем остатке денежных средств на них, а также формировать отчет о движении денежных средств по этим счетам за выбранный период (текущим счетам, текущим счетам с использованием банковских карт, депозитным счетам, кредитам и другим услугам, подключенным клиенту.

8. Порядок обработки Электронных документов

8.1.Создание Электронных документов и подписание их Электронной подписью Клиента осуществляется средствами Системы «iBank2». При невозможности создания Электронного документа или подписания его Электронной подписью в Системе «iBank2» Клиент вправе осуществлять операции по своим счетам в общем порядке в соответствии с заключенным договором банковского счета.

8.2.При сохранении Электронного документа он автоматически размещается на сервере Системы «iBank2» (на стороне Банка), однако до подписания Клиентом юридической силы не имеет (находится в статусе «Новый»). Клиент имеет возможность ознакомиться с созданным Электронным документом, а также вправе отклонить (не подписывать) и удалить созданный документ до подписания.

8.3.Неподписанные или не прошедшие проверку Электронной подписи Электронные документы к дальнейшей обработке не принимаются.

8.4.Банк не осуществляет контроль за содержанием в Электронном документе информации, указанной Клиентом в полях «Номер телефона», «Номер договора», «Номер лицевого счета» и в иных подобных полях. Контроль за содержанием поля «Сумма платежа» Банк осуществляет исключительно с целью проверки достаточности денежных средств на счете Клиента для осуществления платежа и списания комиссионного вознаграждения Банку согласно Тарифам.

8.5.В случае перечисления средств по ошибочным реквизитам или ошибочного перечисления средств в излишнем объеме Клиент самостоятельно принимает меры по возврату денежных средств от получателя.

8.6.Электронный документ, прошедший проверку Электронной подписи и иные проверки в соответствии с настоящими Правилами, принимается к исполнению.

8.7.Электронный документ, не прошедший проверку Электронной подписи и иные проверки в соответствии с настоящими Правилами, не принимается к исполнению. Об отказе в приеме к исполнению Электронного документа Банк информирует Клиента путем изменения статуса Электронного документа в Системе «iBank2» на «Отвергнут».

Дополнительно Банк может уведомляет Клиента об отказе в исполнении Электронного документа путем направления SMS/PUSH-уведомления об изменении статуса документа на «Отвергнут».

8.8.Исполнение Банком Электронных документов Клиента, прошедших проверку в соответствии с настоящими Правилами, и перечисление денежных средств со счета осуществляется не позднее следующего рабочего дня после поступления Электронного

документа в Банк при выполнении настоящих Правил, действующего законодательства Российской Федерации и в соответствии с Регламентом работы в Системе «iBank2» (Приложение №2 к настоящим Правилам).

8.9.Об исполнении Электронного документа Банк информирует Клиента в порядке, предусмотренном пунктом 9.1. настоящих Правил.

8.10.Клиент может по каким-либо причинам отозвать полученный Банком, но еще не исполненный Электронный документ Клиента. Для этого необходимо сделать следующее:

- в максимально короткий промежуток времени направить по Системе «iBank2» (в разделе «Почта» выбрать меню «Рабочие» и нажать ссылку «Создать новое письмо») Заявление об отзыве платежа, подписанное Электронной подписью, в котором указываются реквизиты отзываемого Электронного документа (Приложение № 11);
- после отправки Заявления об отзыве платежа Клиенту необходимо немедленно связаться с сотрудником подразделения Банка, в котором открыт Счет и дополнительно сообщить о факте отправки такого письма.

8.11.Заявление об отзыве платежа служит основанием для возврата (аннулирования) Банком Электронного документа.

8.12.Банк не позднее рабочего дня, следующего за днем поступления Заявления об отзыве платежа, направляет Клиенту по Системе «iBank2» уведомление в виде электронного письма с указанием возможности (невозможности в связи с наступлением безотзывности перевода денежных средств) отзыва платежа.

8.13.Об исполнении (отказе в исполнении) Заявления об отзыве платежа Банк информирует Клиента в соответствии с п.п. 8.7.- 8.9. настоящих Правил.

8.14.Неисполненные Электронные документы, переданные в целях осуществления перевода денежных средств, возвращаются (аннулируются) Банком не позднее рабочего дня, следующего за днем, в который возникло основание для возврата (аннулирования) Электронного документа, включая Заявление об отзыве платежа.

9. Порядок уведомления Клиента о проводимых операциях по счету

9.1.В соответствии с Федеральным Законом № 161-ФЗ от 27.06.2011г. «О национальной платежной Системе» Банк исполняет свои обязанности по уведомлению Клиента о совершении каждой операции по банковскому счету Клиента с использованием Системы «iBank2», о факте приостановлении или прекращении использования электронного средства платежа с указанием причины такого приостановления или прекращения – в день приостановления (прекращения) следующими способами:

- по операциям, совершенным с использованием Системы «iBank2» осуществляется направление SMS/PUSH-уведомления на номер мобильного телефона, указанный Клиентом. В SMS/PUSH - уведомлении указываются, наименование операции, сумма операции, счет получателя, статус исполнения операции, в случае приостановления (прекращения) исполнения электронного средства платежа – дата, причины такого приостановления (прекращения) и другие данные по усмотрению Банка;
- путем изменения статуса Электронного документа в Системе «iBank2» в разделе «История операций» системы.

9.2. Обязанность Банка по направлению Клиенту уведомлений, предусмотренных пунктом 9.1. настоящих Правил, в соответствии с действующим законодательством, считается исполненной при направлении SMS/PUSH -уведомления на номер мобильного телефона Клиента, указанного в Заявлении. При этом Клиент обязуется не реже чем два раза в день самостоятельно проверять полученные SMS/PUSH-уведомления по указанным в Заявлении средствам связи для контроля операций, проводимых по банковскому счету Клиента с использованием Системы «iBank2».

9.3.При осуществлении уведомления о каждой операции по Счету с использованием Системы «iBank2» несколькими способами Банк считается выполнившим требование законодательства об информировании Клиента о совершении каждой операции с использованием электронного средства платежа с момента уведомления Клиента о соответствующей операции хотя бы одним из способов, предусмотренных п. 9.1. настоящих Правил.

9.4.Уведомление Клиентом Банка о Событии компрометации осуществляется незамедлительно после обнаружения факта утраты электронного устройства, с которого

осуществляется вход в Систему «iBank2», компрометации Авторизационных данных и (или) их использования без согласия Клиента, но не позднее дня, следующего за днем получения из Банка Уведомления:

9.4.1.Клиент уведомляет Банк о Событии компрометации по телефонам (863) 287-00-58, (812) 456-04-05, 8 (800)777 70 01) (прием звонков обеспечивается в рабочие дни с 09:00 до 18:00 по Московскому времени, в дни, предшествующие праздничным и выходным с 09:00 до 17:00 по Московскому времени).

9.4.2.В кратчайшие сроки, но не позднее рабочего дня, следующего за днем обращения по телефону согласно п. 9.4.1, Клиент направляет письменное уведомление по форме, установленной Правилами, путем обращения в Банк.

9.4.3.При условии выполнения обязанности уведомления Банка согласно п.п. 9.4.1 и 9.4.2, временем уведомления Банка считается время завершения телефонного звонка, состоявшегося согласно п. 9.4.1.

9.4.4.В случае уведомления Банка только в письменной форме (п. 9.4.2) временем уведомления считается 15 часов 00 минут (по Московскому времени) рабочего дня, следующего за днем получения Банком письменного уведомления.

9.4.5.Обращение Клиента в Банк только по телефону (п. 9.4.1), без направления письменного уведомления (согласно п. 9.4.2) считается не надлежащим уведомлением Банка о Событии компрометации.

9.4.6. Банк считается надлежаще исполняющим требования Положения Банка России от 17.04.2019 №683-П при подтверждении Клиентом совершенной банковской операции в Системе «iBank2» в порядке, указанном в пункте 11.2.12. настоящего Положения.

10. Права и обязанности Банка

10.1.**Банк обязан:**

10.1.1.Принимать от Клиента по каналам связи Электронные документы при условии их правильного оформления и подписания Электронной подписью Клиента.

10.1.2.На основании полученного от Клиента Уведомления в письменном виде (Приложения № 6) или посредством телефонной связи, после произнесения Клиентом Блокировочного слова:

- блокировать в Системе «iBank2» Учетную запись Клиента;

На основании полученного от Клиента собственноручно подписанного соответствующего Уведомления (Приложение № 7):

- активировать ранее заблокированную Учетную запись;

10.1.3.Уведомлять Клиента о совершении каждой операции, проводимой по банковскому счету Клиента с использованием Системы «iBank2», путем направления Клиенту соответствующего SMS/PUSH-уведомления в порядке, определенном в разделе 9 настоящих Правил.

10.1.4.Предоставлять по требованию Клиента документы и информацию, которые связаны с использованием Клиентом Системы «iBank2»:

- на бумажном носителе в виде выписки по счету, предоставляемой в офисах Банка;
- иные документы на основании заявления Клиента, составленного им в произвольной форме.

10.1.5.Регистрировать и хранить в течение не менее 3 лет протоколы действий Клиента в Системе «iBank2». Протоколы операций Клиента имеют гриф «Конфиденциально» и являются конфиденциальной информацией Банка. В случае компрометации ключевой информации системы «iBank2» Банк имеет право отказать Клиенту в предоставлении данной информации по письменному или устному заявлению Клиента. Протоколы операций могут быть выданы только по решению суда либо по письменному запросу правоохранительных органов при урегулировании споров.

10.1.6.Рассматривать заявления Клиента, в том числе при возникновении споров, связанных с использованием Клиентом Системы «iBank2», а также предоставить Клиенту возможность получать информацию о результатах рассмотрения заявлений, в том числе в письменной форме по требованию Клиента, в срок не более 30 дней со дня получения таких заявлений, а также не более 60 дней со дня получения заявлений в случае использования Системы «iBank2» для осуществления трансграничного перевода денежных средств.

10.1.7. Уведомить Клиента о выявлении операции, соответствующей признакам совершения перевода денежных средств без согласия клиента по номеру телефона, указанного в Заявлении о присоединении к Правилам предоставления дистанционного банковского обслуживания.

10.1.8. Предоставить клиенту информацию о рекомендациях по снижению рисков повторного совершения операции, соответствующей признакам совершения перевода денежных средств без согласия клиента.

10.1.9. Аннулировать совершение приостановленного перевода денежных средств, выявленного в ходе мониторинга операций, соответствующих признакам совершения перевода денежных средств без согласия клиента, если клиент опроверг легитимность операции.

10.1.10. Отменить приостановку использование Клиентом Системы «iBank2» при подтверждении Клиентом операции, соответствующей признакам совершения перевода денежных средств без согласия клиента.

10.1.11. Исполнить распоряжение Клиента при подтверждении Клиентом операции, соответствующей признакам совершения перевода денежных средств без согласия клиента.

10.2.**Банк имеет право:**

10.2.1.Без объяснения причин отказать Клиенту в заключении настоящего Договора.

В случае компрометации либо подозрения в компрометации Авторизационных данных Клиента, если, по мнению Банка, такие меры необходимы для обеспечения безопасной работы в Системе:

- блокировать Учетную запись Клиента;
- потребовать от Клиента смену пароля для доступа в Систему.

10.2.2.Потребовать от Клиента собственноручно подписать и предоставить не позднее рабочего дня, следующего за датой требования, документ на бумажном носителе, эквивалентный по смыслу и содержанию Электронному документу, ранее поступившему в Банк по Системе «iBank2».

10.2.3.Потребовать от Клиента собственноручно подписать и предоставить в Банк оформленные в соответствии с требованиями Банка России документы, необходимые для исполнения Электронного документа в соответствии с действующим законодательством.

10.2.4.Отказать Клиенту в исполнении Электронного документа, поступившего по Системе «iBank2», уведомив его (в соответствии с п.8.7 настоящих Правил) не позднее рабочего дня, следующего за днем получения такого Электронного документа, в следующих случаях:

- Электронная подпись Клиента неверна;
- в случае недопустимости и несоответствия значений реквизитов Электронного документа;
- на счете Клиента отсутствуют денежные средства, необходимые для проведения соответствующей операции;
- превышен Лимит (суточный/месячный) на суммы проводимых операций по счету Клиента;
- на счете Клиента отсутствуют денежные средства, необходимые для списания комиссии после проведения соответствующей операции. Отказать Клиенту в отзыве Электронного документа, переданного в целях осуществления перевода денежных средств, в связи с наступлением безотзывности перевода денежных средств.

10.2.5.Запрашивать у Клиента по Системе «iBank2» документы и сведения, необходимые Банку для фиксирования информации в соответствии с нормами действующего законодательства Российской Федерации в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма. Указанные запросы, направленные в виде ЭД, имеют юридическую силу официальных писем Банка.

Все ЭД, поступившие Клиенту по Системе «iBank2» считаются полученными и прочитанными Клиентом. В случае непредставления Клиентом в указанный в запросе Банка срок документов и сведений, Банк вправе отказать клиенту в приеме от него распоряжения на проведение операции по банковскому счету (вкладу), подписанного Электронной подписью, предварительно уведомив Клиента в письменной форме до осуществления указанных мероприятий. После уведомления Банк принимает от Клиента только надлежащим образом оформленные расчетные документы на бумажном носителе.

10.2.6.Отказать Клиенту в использовании системы «iBank2» в случае, если у сотрудников Банка возникают подозрения, что операции по счетам совершаются в целях легализации

(отмывания) доходов, полученных преступным путем, или финансирования терроризма. Банк, в случае выявления сомнительных операций Клиента, вправе после предварительного письменного предупреждения, отказать Клиенту в приеме от него распоряжений, подписанных Электронной подписью, с последующим принятием от такого Клиента только надлежащим образом оформленных расчетных документов на бумажном носителе.

10.2.7.Отказать Клиенту в выполнении распоряжения на проведение операции по счету, подписанного Электронной подписью на основании пункта 11 статьи 7 Федерального закона от 07.08.2001г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». Уведомление о принятом решении об отказе в выполнении распоряжения о совершении операции направляется Клиенту в день принятия такого решения по Системе «iBank2».

10.2.8.Приостановить использование Клиентом Системы «iBank2» до 2х рабочих дней при выявлении операций, соответствующих признакам совершения перевода денежных средств без согласия Клиента.

10.2.9.Приостановить исполнения распоряжения Клиента до 2х рабочих дней, соответствующих признакам совершения перевода денежных средств без согласия Клиента.

10.2.10.Запросить у Клиента подтверждение легитимности выявленной операции, соответствующей признакам совершения перевода денежных средств без согласия Клиента

11. Права и обязанности Клиента

11.1.**Клиент имеет право:**

11.1.1.Лично или по средствам телефонной связи, после произнесения Блокировочного слова, блокировать в Системе свою Учетную запись.

11.1.2.Снять блокировку Учетной записи, предоставив в Банк собственноручно подписанное Уведомление (Приложение № 7) на снятие такой блокировки.

По своему усмотрению

- изменять отображение счетов, номер контактного телефона путем подачи соответствующего заявления в письменном виде (Приложение № 10) или в электронном виде по Системе (в случае предоставления такой возможности Банком);
- изменять Блокировочное слово путем направления в Банк письменного заявления по форме Приложения № 10.

11.1.3.Самостоятельно в любое время и неограниченное количество раз изменять свой Пароль доступа к Системе.

11.1.4.Требовать от Банка предоставления документов и информации, которые связаны с использованием Клиентом Системы «iBank2»:

- на бумажном носителе в виде выписки по счету, предоставляемых в офисах Банка;
- иные документы на основании заявления Клиента, составленного им в произвольной форме.

11.1.5.Отозвать еще не исполненный Банком Электронный документ до момента наступления безотзывности перевода денежных средств.

11.1.6.Получать консультации по вопросам работы Системы «iBank2» и по вопросам совершения операций в Системе по телефонам (863) 287-00-58, (812) 456-04-05, 8 (800)777 70 01 (в рабочее время).

11.2.**Клиент обязан:**

11.2.1. Хранить в секрете и не передавать третьим лицам Авторизационные данные, SIM-карту с номером мобильного телефона, указанным Клиентом в Заявлении, который используется для получения кодов, паролей, а также Блокировочное слово.

11.2.2.По требованию Банка собственноручно подписать и предоставить не позднее рабочего дня, следующего за датой требования, документ на бумажном носителе, эквивалентный по смыслу и содержанию Электронному документу, ранее поступившему в Банк по Системе «iBank2».

11.2.3.По требованию Банка собственноручно подписать и предоставить в Банк оформленные в соответствии с требованиями Банка России документы, необходимые для исполнения Электронного документа в соответствии с действующим законодательством Российской Федерации.

11.2.4.В случае утраты SIM-карты с номером мобильного телефона, который указан в Заявлении, и (или) их использования без согласия Клиента Клиент обязан сообщить об этом в

Банк по средствам телефонной связи и направить в Банк соответствующее Уведомление (Приложения №6, №7 к настоящим Правилам) незамедлительно после обнаружения факта утраты и (или) использования без согласия Клиента, но не позднее дня, следующего за днем обнаружения факта утраты и (или) получения от Банка уведомления о совершенной операции с использованием Системы «iBank2».

11.2.5.В случае утраты или компрометации Блокировочного слова незамедлительно сообщить об этом в Банк по средствам телефонной связи и изменить его в соответствии с п. 12.1.3 настоящих Правил.

11.2.6. По запросу Банка представлять информацию, необходимую для исполнения Банком требований, предусмотренных нормами действующего законодательства Российской Федерации в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма:

- документы и сведения, раскрывающие экономический смысл проводимой операции;
- документы и сведения, необходимые Банку для идентификации Клиента, его представителя, бенефициарного владельца и выгодоприобретателя, в том числе, в случае изменения ранее предоставленных сведений;
- иные сведения и документы по запросу Банка.

11.2.7.Не реже двух раз в день путем формирования выписки по Счету в Системе «iBank2» осуществлять контроль состояния своих счетов (даже, если операции по счетам не проводились), а также осуществлять просмотр информации, переданной Клиенту Банком посредством Системы «iBank2».

11.2.8. Сообщить в Банк информацию согласно п. 9.4.1 и п. 9.4.2 о выявлении операции совершения перевода денежных средств без согласия Клиента.

11.2.9.Надлежащим образом выполнять все рекомендации Банка по использованию Системы «iBank2», указанные в Приложениях №3, №5 к Правилам.

11.2.10.На протяжении действия настоящего Договора использовать лицензионное антивирусное программное обеспечение с настройками, позволяющими поддерживать антивирусные базы данных в актуальном состоянии.

11.2.11.Своевременно информировать Банк в письменном виде об изменениях данных документа, удостоверяющего личность, адреса места жительства (пребывания), предоставлять обновленную информацию для связи с Клиентом и другие сведения, необходимые для обслуживания Клиента в Системе «iBank2», в течение 3 (Трех) рабочих дней с момента таких изменений.

11.2.12. Отслеживать статус своего Электронного документа в Системе «iBank2». В случае, если Клиент в течение 15 минут после совершения операции, т.е после изменения статуса Электронного документа в Системе «iBank2 на статус «Исполнен», не уведомит Банк способом, указанным в пункте 9.4 настоящих Правил о своем несогласии с совершенной операцией, операция в Системе «iBank2» считается подтвержденной Клиентом в рамках требований Положения Банка России от 17.04.2019 №683-П.

12. Совместные обязательства и ответственность Сторон

12.1. Клиент несет ответственность и принимает все риски за последствия, возникшие вследствие несоблюдения Клиентом рекомендаций Банка, указанных в Приложении № 3 к настоящим Правилам.

12.2.Клиент несет ответственность за полноту, достоверность и своевременность предоставленной персональной информации для заключения Договора и обслуживания в Системе «iBank2» в соответствии с действующим законодательством РФ.

12.3.Клиент несет ответственность за убытки, возникшие вследствие исполнения Банком Электронного документа Клиента, составленного с ошибками в информации, содержащейся в полях Электронного документа, и на сумму, превышающую сумму ежемесячного платежа Клиента получателю денежных средств.

12.4.Банк несет ответственность за сохранность денежных средств на счетах Клиента, подключенных к Системе «iBank2», при соблюдении Клиентом условий настоящих Правил.

12.5.Банк не несет ответственность за неисполнение Электронного документа Клиента, если его исполнение привело бы к нарушению требований действующего законодательства РФ, нормативных актов Банка России, настоящих Правил, условий иных заключенных между

Клиентом и Банком соглашений (договоров), в том числе, если процедура приема к исполнению Электронного документа Клиента дала отрицательный результат.

12.6. Банк не несет ответственности:

12.6.1. За неисполнение распоряжения Клиента, если:

- исполнение зависит от определенных действий третьей стороны, и невыполнение или несвоевременное выполнение связано с тем, что третья сторона не может или отказывается совершить необходимые действия, совершает их с нарушениями установленного порядка или недоступна для Банка;
- неисполнение явилось следствием непреодолимой силы, то есть чрезвычайных и непредотвратимых при данных условиях обстоятельств, возникших после заключения настоящих Правил. Действие обстоятельств непреодолимой силы Стороны должны подтверждать документами компетентных органов. О наступлении обстоятельств непреодолимой силы Стороны обязуются извещать друг друга в пятидневный срок.

12.6.2.За неоказание, несвоевременное оказание третьей стороной услуг, оплаченных Клиентом через Систему.

12.6.3.За убытки, понесенные Клиентом, вследствие исполнения Банком распоряжения Клиента, составленного с ошибками в представленной Банку информации.

12.6.4.За убытки, понесенные Клиентом, вследствие нарушения Клиентом порядка использования Системы, установленного в настоящих Правилах, в Памятке по использованию системы, а также в инструкциях, размещенных на официальном сайте Банка в сети Интернет по адресу: www.rostfinance.ru.

12.6.5.За аварии, сбои или перебои в обслуживании, связанные с нарушением в работе оборудования, систем подачи электроэнергии и/или линий связи или сетей, которые обеспечиваются, подаются, эксплуатируются и/или обслуживаются третьей стороной.

12.6.6.За действия Клиента в Системе, подтвержденные корректным вводом разового пароля, переданного Банком/сформированного устройством/генератором паролей.

12.6.7.По операциям, совершенным по банковскому счету/счету по вкладу Клиента, вследствие неполучения/несвоевременного получения Клиентом SMS- уведомлений не по вине Банка.

12.6.8.За несанкционированное использование третьими лицами информации, указанной в SMS/PUSH -уведомлении, в случае если данная информация стала известна третьим лицами не по вине Банка.

12.7.Банк не несет ответственность за неполучение Клиентом информации, связанной с использованием Системы «iBank2», если контактные данные, переданные в Банк Клиентом стали неактуальными, информация, о чем не была доведена Клиентом до Банка своевременно и в установленном Банком порядке.

12.8.Банк не несет ответственности, если информация об изменении Правил и (или) Тарифов, опубликованная в порядке и в сроки, установленные Правилами, не была получена и изучена и (или) правильно истолкована Клиентом.

12.9.До момента расторжения Договора Стороны несут ответственность по всем Электронным документам с Электронной подписью Клиента, принятым Банком по Системе «iBank2», в соответствии с действующим законодательством РФ.

12.10.В случае возникновения конфликтных ситуаций между Клиентом и Банком при использовании Системы «iBank2» Стороны обязуются участвовать в рассмотрении конфликтов в соответствии с положением «О порядке проведения технической экспертизы при возникновении спорных ситуаций» (Приложением № 4 к настоящим Правилам), выполнять требования указанного положения и нести ответственность согласно выводам по рассмотрению конфликтной ситуации.

12.11.Стороны обязуются при разрешении экономических и иных споров, которые могут возникнуть в связи с использованием Системы «iBank2», предоставлять в письменном виде свои оценки, доказательства и выводы по запросу заинтересованной стороны, участвующей в настоящем Договоре.

12.12.Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение взятых по настоящему Договору обязательств в случае возникновения обстоятельств непреодолимой силы, к которым относятся: стихийные бедствия, пожары, аварии, отключения электроэнергии, повреждение линий связи, массовые беспорядки, забастовки, военные действия, противоправные действия третьих лиц, а также технические неисправности, возникших по вине

третьих лиц, вступление в силу законодательных актов, актов федеральных или местных органов власти и обязательных для исполнения одной из Сторон, прямо или косвенно запрещающих указанные в Договоре виды деятельности или препятствующие выполнению Сторонами своих обязательств по Договору. При этом срок исполнения обязательств отодвигается соразмерно времени, в течение которого действовали такие обстоятельства, если исполнение обязательств остается возможным.

13. Финансовые отношения

13.1. Подключение Клиента к Системе, выполнение действий по Регистрации Клиента, его Авторизационных данных, устройств получения и генерации ключевой информации и Ключей электронной подписи, подключение Клиенту дополнительных услуг Системы производится только после взимания Банком установленной платы в соответствии с Тарифами.

13.2.Клиент предоставляет Банку право (дает предварительный акцепт) на списание платы за подключение и обслуживание в Системе, включая дополнительные услуги Системы, в соответствии с Тарифами без дополнительного распоряжения Клиента, со Счета Клиента, указанного в заявление о присоединении к настоящим Правилам.

13.3.В случае неисполнения Клиентом своих обязательств по оплате обслуживания в Системе Банк вправе произвести отключение соответствующих услуг (отключение производится Банком после 10 числа месяца, за который не внесена предусмотренная плата).

13.4.При расторжении Договора уплаченная Банку плата Клиенту не возвращается.

14. Срок действия Договора

14.1.Настоящий Договор вступает в силу с момента регистрации в Банке Заявления о присоединении к Правилам.

14.2.Действие Договора не ограничено сроком.

14.3.Договор может быть расторгнут в одностороннем порядке по требованию одной из Сторон:

14.3.1.По инициативе Клиента в любое время по его письменному заявлению по форме Приложения № 9. Банк прекращает предоставление услуг с даты регистрации заявления, в том числе блокирует доступ Клиента к Системе и аннулирует Авторизационные данные Клиента.

14.3.2.По инициативе Банка:

- при нарушении Клиентом Правил, на основании письменного уведомления, уведомления через систему «iBank2», СМС оповещения, направленного Клиенту за 10 (Десять) календарных дней до планируемой даты прекращения обслуживания. По истечении 10 (Десяти) календарных дней Банк прекращает предоставление услуг, в том числе блокирует доступ Клиента к Системе и аннулирует Авторизационные данные Клиента.
- в случае, если в течение 90 (Девяноста) календарных дней подряд с момента регистрации Клиента в Системе «iBank2», Клиент не выполнил ни одного входа в Систему на основании письменного уведомления, уведомления через систему «iBank2», СМС оповещения, направленного Клиенту за 10 (Десять) календарных дней до планируемой даты прекращения обслуживания. По истечении 10 (Десяти) календарных дней Банк прекращает предоставление услуг, в том числе блокирует доступ Клиента к Системе и аннулирует Авторизационные данные Клиента.

15. Заключительные положения

15.1. Споры по настоящему Договору решаются путем переговоров с учетом взаимных интересов (в том числе в соответствии с Приложением № 4 к настоящим Правилам), а при не достижении соглашения – в судебном порядке.

15.2. Банк извещает Клиента об изменениях Правил и (или) Тарифов за 10 (Десять) рабочих дней до даты их введения в действие путем размещения информации на информационных стендах в подразделениях Банка и на сайте Банка в сети Интернет (www.rostfinance.ru), а также иными способами, указанными в п.2.6 настоящих Правил.

15.3.Клиент вправе согласиться с предложенными изменениями к Правилам и (или) Тарифам (акцептовать) любым из следующих способов:

- путем направления Банку письменного подтверждения согласия (акцепта) на вносимые в Правила и (или) Тарифы изменения в виде документа на бумажном носителе, подписанного собственноручно, или в виде Электронного документа с Электронной

подписью либо непредставлении Банку письменного отказа в их изменении и (или) Заявления о расторжении Договора в порядке, установленном в разделе 14 настоящих Правил;

- путем предоставления с даты направления Банком предложения (оферты) Банка на изменение к Договору и (или) Тарифам Электронных документов, свидетельствующих о намерении Клиента исполнять Договор с учетом изменений.

15.4.Договор и (или) Тарифы считаются измененными по соглашению Сторон по истечении 10 (Десяти) рабочих дней после публикации сообщения (оферты) об изменениях на сайте Банка при условии, что в течение этого срока Банк не получит от Клиента письменного Заявления о расторжении Договора.

15.5.Клиент обязан не реже 1 (Одного) раза в 5 (Пять) календарных дней знакомиться с информацией, публикуемой Банком в соответствии с п. 2.6 настоящих Правил.

15.6.В случае несогласия Клиента с планируемыми изменениями в Правила или Тарифы Клиент вправе расторгнуть Договор в порядке, установленном в разделе 17 настоящих Правил.

15.7.В случае если Клиент выразил свое согласие на обработку его персональных данных, Банк осуществляет обработку персональных данных Клиента в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных».

15.8.Все протоколы операций, совершенные Клиентом с использованием Системы «iBank2» имеют юридическую силу, как и заключенные Правила, между Банком и Клиентом.

15.9.Клиент предоставляет согласие на проведение аудиозаписи телефонных переговоров между Клиентом и Банком. Стороны признают, что указанные аудиозаписи могут быть использованы в суде в качестве доказательств в соответствии со ст. 55 Гражданского процессуального кодекса Российской Федерации.

Приложение № 1
к Правилам дистанционного банковского обслуживания
физического лица в Системе «iBank2»

ЗАЯВЛЕНИЕ №__ _____ от _____201

о присоединении к Правилам предоставления дистанционного банковского обслуживания для физических лиц в ООО КБ «РостФинанс»

1. Ф.И.О. клиента_____
2. Арес регистрации
   Адрес места жительства
3. Тел.___ 4. ИНН _____
5. Факс_____ 6. E-mail_____

7. Документ, удостоверяющий личность _____, серия _____ номер _____,
   дата выдачи «___»_____20__г., кем выдан _____
_____
Логин в Системе «iBank2» (заполняется после Регистрации в Системе) _____

1.Прошу подключить к Системе «iBank2» Все счета, открытые на мое имя в ООО» КБ РостФинанс»

2. Блокировочное слово

Блокировочное слово (для идентификации, при обращении в Банк по телефону, с просьбой о временном блокировании работы в Системе):

_____

3.Номер мобильного телефона для получения уведомлений по Системе «iBank2»

+7												*

Настоящим сообщаю, что с Тарифами комиссионного вознаграждения по обслуживанию физических лиц Банка, Правилами предоставления дистанционного банковского обслуживания для физических лиц в ООО КБ «РостФинанс» (далее - Правила), являющимися договором присоединения в соответствии со ст. 428 Гражданского кодекса Российской Федерации, я ознакомлен (а), присоединяюсь к ним, согласен(на) с ними и обязуюсь неукоснительно соблюдать. Условия мною получены, их положения разъяснены.

Согласен(а) с тем, что обязанность Банка по информированию Клиента о совершенных операциях по счетам с использованием Системы считается исполненной в момент отправки соответствующего SMS/PUSH-уведомления на указанный в настоящем Заявлении номер мобильного телефона . Банк не несет ответственности за отсутствие у Клиента доступа к средствам связи, с использованием которых Клиент может получить SMS/PUSH -уведомление, либо несвоевременное получение SMS/PUSH -уведомления, в том числе за сбои в работе Интернета, сетей связи, возникшие по независящим от Банка причинам и повлекшие за собой несвоевременное получение или неполучение Клиентом SMS/PUSH - уведомлений Банка.

Согласие клиента

В соответствии с Федеральным законом № 152-ФЗ «О персональных данных» от 27.07.06г. я выражаю свое Согласие Банку на обработку своих персональных данных (сбор, систематизацию, накопление, хранение, уточнение, использование, распространение (передачу определенному кругу лиц), блокирование, уничтожение) как с использованием средств автоматизации, так и без использования таких средств в целях продвижения на рынке услуг Банка, предусмотренных настоящими Правилами, а также с целью маркетинговых исследований. Подтверждаю, что, давая такое Согласие, я действую своей волей и в своем интересе.

Согласие дается мною для целей оказания мне банковских услуг и исполнения Банком моих поручений как на основании заключенных договоров, так и без таковых, а также с целью заключения, исполнения и расторжения договоров между мной и Банком и в соответствии с целями, указанными в таких договорах. Перечень персональных данных, на обработку которых дается настоящее согласие включает в себя любую информацию, предоставляемую мной в настоящем Заявлении и других представляемых в Банк документах.

Настоящее согласие дается на сроки хранения соответствующей информации в соответствии с Законодательством РФ и внутренними документами Банка, а также на срок, необходимый для достижения установленных в настоящем согласии целей и может быть отозвано путем направления мною соответствующего письменного уведомления Банку.

* Настоящим Клиент подтверждает принадлежность ему указанного номера мобильного телефона и согласие на получение Одноразовых паролей на мобильный телефон с вышеуказанным номером.

С действующими Тарифами Банка, лимитами и ограничениями в Системе «iBank2» и приложении «Мобильный банк» на момент подписания настоящего Заявления ознакомлен(а) и согласен(а)*

Клиент:

_____/_____ /
(подпись) (фамилия, имя отчество полностью)

Отметки Банка: Договору «____»_____201__г. присвоен №_____

О принятии заявления:

Должность сотрудника Банка	ФИО	Дата	Подпись

О подключении:

Должность сотрудника Банка	ФИО	Дата	Подпись

Приложение № 2
к Правилам дистанционного банковского обслуживания
физического лица в Системе «iBank2»

РЕГЛАМЕНТ
работы в Системе «iBank2»

Банк принимает Электронные документы, переданные по Системе «iBank2», круглосуточно. Исполнение Электронных документов, переданных по Системе «iBank2», осуществляется ежедневно (кроме субботы и воскресенья) по следующему расписанию:

Переводы в другие банки, переводы между клиентами внутри банка, переводы по своим счетам в разных Филиалах

Рубли РФ	**Понедельник-четверг**	**9:30 - 17:00**
	Пятница	**9:30 - 16:00**

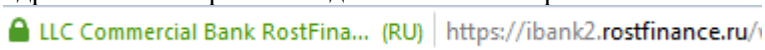
Документы, поступившие в Банк позже указанного времени, исполняются на следующий рабочий день.

Переводы по своим счетам, переводы на карту внутри банка и оплата услуг в валюте счета – круглосуточно.

Переводы по своим счетам с конвертацией валют – ежедневно с 9:00 до 16:00

Приложение № 3
к Правилам дистанционного банковского обслуживания
физического лица в Системе «iBank2»

РЕКОМЕНДАЦИИ
по мерам безопасности при работе в Системе «iBank2»

1. Рекомендуем для работы в Системе «iBank2» выделить отдельное ЭУ, с которого не будет производиться других подключений к сети Интернет.
2. Вход в Систему «iBank2» необходимо осуществлять через сайт Банка www.rostfinance.ru в разделе «Вход в Интернет-Банк» далее «Для физических лиц».
3. Убедиться, что адрес сайта Системы «iBank2» имеет защищенное соединение: адрес сайта Системы обязательно должен начинаться с «**https»** (s означает «secure» защищенное); в адресной строке должен отображаться символ закрытого замка. 

4. После входа на стартовую страницу Системы «iBank2» проверьте корректность сертификата безопасности, нажатием на символ закрытого замка – «Просмотреть сертификат».
5. Используйте только доверенные электронные устройства (далее ЭУ) с лицензионным программным обеспечением, установленным и запущенным антивирусным программным обеспечением (ПО) и персональным межсетевым экраном, своевременно обновляйте антивирусные базы. Регулярно проводите полную проверку компьютера на предмет наличия вредоносного ПО, своевременно обновляйте лицензионную операционную систему и браузеры. Используя для работы в Системе незащищенное антивирусными программами ЭУ, Вы потенциально подвергаетесь угрозе хищения Авторизационных данных вредоносной программой (например, «Трояном»).
6. Для входа в Систему вам требуется вводить только ваш логин и пароль. Не нужно вводить номер вашего мобильного телефона, номер вашей банковской карты или CVV2/CVC2 код для входа или дополнительной проверки персональной информации в Системе. Рекомендуется использовать виртуальную клавиатуру для ввода пароля.
7. При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходить по содержащимся в таких письмах ссылкам.
8. Не сообщайте никому свои Авторизационные данные, код активации Учетной записи, Блокировочное слово, SMS-код, используемый для подписания Электронного документа, а также номера ваших карт и CVV2/CVC2 коды.
9. Регулярно производите смену пароля. Банк рекомендует производить смену пароля с регулярностью каждые 90 дней.
10. Не используйте пароль, используемый в Системе «iBank2» в любых других системах и сервисах.
11. Не оставляйте мобильный телефон (SIM-карту), используемый для получения SMS-кода, без присмотра в местах, доступных для третьих лиц, и никому не передавайте.
12. При работе в Интернет не соглашаться на установку каких-либо дополнительных программ от недоверенных издателей.
13. Отключите в настройках браузера автозаполнение (запоминание) логинов и паролей для сайтов и запоминание истории Вашей работы с web-сайтами.
14. Просматривайте журнал «Сеансы работы» (показывается автоматически при входе в Систему «iBank2») на предмет подозрительных сеансов связи. Обращайте внимание на дату и время последних входов в систему (данные фиксируются на первой странице после входа в Систему).
15. При завершении работы в Системе «iBank2» всегда нажимайте кнопку «Выход».
16. Устанавливайте мобильные приложения ООО КБ «РостФинанс» БИФИТ только из авторизованных магазинов App Store и Google Play. Перед установкой приложения убедитесь, что их разработчиком является БИФИТ. Используйте антивирусное программное обеспечение, в случае, если оно доступно для вашего электронного устройства.
17. Обязательно сверяйте текст SMS-сообщений, содержащий пароль, с деталями выполняемой вами операции. Если в SMS указан пароль для платежа, который вы не

совершали или вам предлагают его ввести/назвать, чтобы отменить якобы ошибочно проведенный по вашему счету платеж, ни в коем случае не вводите его в Интернет-банке и не называйте его, в том числе сотрудникам банка.

18. При доступе с гостевых рабочих мест (Интернет-кафе и т.д.) увеличивается риск хищения и дальнейшего неправомерного использования авторизационной информации. В связи с этим осуществляйте доступ к Системе «iBank2» только со своего ЭУ в целях сохранения и конфиденциальности персональных данных и (или) информации о банковском счете.
19. Подключите у Интернет-провайдера услугу «фиксированный IP – адрес» и через Управление автоматизации информационных систем Банка зарегистрируйте его в Системе «iBank2». В этом случае Вы исключите возможность работы злоумышленников в Системе «iBank2» от Вашего имени с другого ЭУ.
20. Избегайте регистрации номера вашего мобильного телефона, на который приходят SMS-сообщения с разовым паролем, в социальных сетях и других открытых источниках.
21. В случае если доступ осуществляется с использованием чужого ЭУ, не сохраняйте на нем персональные данные и другую информацию, а после завершения всех операций убедитесь, что персональные данные и другая информация не сохранились (вновь загрузив в браузере web-страницу, с которой осуществлялся доступ).
22. Осуществляйте информационное взаимодействие с Банком только с использованием средств связи (мобильные и стационарные телефоны, факсы, web-сайты, обычная и электронная почта и пр.), реквизиты которых оговорены в документах, получаемых непосредственно в Банке.
23. При обмене с Банком не может выдаваться никаких предупреждений, например, «До 9:00 в банке профилактика, попробуйте позже». При появлении необычных сообщений срочно сообщайте в Банк!

<u>При возникновении следующих ситуаций, просим незамедлительно обращаться в Банк, с целью оперативного блокирования доступа:</u>

24. На компьютере или электронном устройстве, используемом для работы в Системе, обнаружено вредоносное ПО (вирусы, «трояны» и т.д.).
25. В «Журнале сеансов работы» обнаружены факты проникновения в систему посторонних лиц (вход в систему с нетипичного IP-адреса либо в нетипичное для Вас время).
26. В выписке обнаружены несанкционированные Вами расходные операции, либо Вы получили SMS уведомление об операции, которую не совершали.
27. Вы получили SMS или e-mail-уведомление об изменении адреса e-mail или номера мобильного телефона для отправки уведомлений, при этом изменения были совершены без Вашего ведома.

<u>Правила в случаи наступления События компрометации</u>

28. Событие компрометации – событие, в результате которого возможно несанкционированное использование электронного ключа подписи. К событиям, связанным с компрометацией ключей относятся, включая, но, не ограничиваясь, следующие:
    - потеря электронного устройства;
    - потеря электронного устройства с его последующим обнаружением;
    - компрометация Авторизационных данных.
29. В случае компрометации электронного ключа подписи Клиент должен немедленно известить об этом Банк по телефону, назвав блокировочное слово, но не позднее дня, следующего за днем получения из Банка уведомления, а также Клиент обязан подать в Банк письменное Уведомление о блокировке /активации /создании Учетной записи в Системе «iBank2» (Приложение № 7 Правил).
30. При установлении факта компрометации электронного ключа подписи должны быть приняты следующие меры:
    - Незамедлительно сообщить о факте компрометации в Банк: +7 (863) 287-00-58, (812) 456-04-05, 8 800 777-70-01.
    - Немедленно прекратить работу в Системе.

31. В случае возникновения любых подозрений на компрометацию Авторизационных данных, SIM-карты, кода активации Учетной записи, Блокировочного слова необходимо

сообщить об этом в Банк по телефонам (863) 287-00-58, (812) 456-04-05, 8 (800)777 70 01 (в рабочее время).

Обращайте повышенное внимание на все отклонения в стандартной работе программно-технических средств рабочего места пользователя Системы «iBank2». При обнаружении отклонений необходимо сразу же сообщить об этом в Банк по телефонам: (863) 287-00-58, (812) 456-04-05, 8 (800)777 70 01 (в рабочее время)

Приложение № 4
к Правилам дистанционного банковского обслуживания
физического лица в Системе «iBank2»

ПОЛОЖЕНИЕ
о порядке проведения технической экспертизы при возникновении спорных ситуаций

1. В настоящем Положении под спорной ситуацией понимается существование претензий у Клиента к Банку, справедливость которых может быть однозначно установлена по результату проверки Электронной подписи Клиента под Электронным документом.
2. Клиент представляет Банку собственноручно подписанное заявление в произвольной форме, содержащее существо претензии с указанием на документ с Электронной подписью, на основании которого Банк выполнил операции по Счету Клиента.
3. Рассмотрение претензий в Банке осуществляется в течение 30 (Тридцати) календарных дней, а в случае, если претензия связана с исполнением Электронного документа, содержащего трансграничный перевод, – в течение 60 (Шестидесяти) календарных дней с даты получения претензии относительно операции по Счету.
4. По итогам рассмотрения и в зависимости от принятого решения Банк либо удовлетворяет претензию Клиента, либо передает Клиенту письменное заключение о необоснованности его претензии, подписанное уполномоченным работником Банка.
5. В случае несогласия с заключением Банка по предъявленной Банку претензии Клиент направляет в Банк письменное уведомление о своем несогласии с требованием о формировании разрешительной комиссии для рассмотрения спора.
6. Банк обязан в течение не более 5 (Пяти) рабочих дней от даты подачи уведомления Клиента о несогласии с заключением Банка по предъявленной Банку претензии сформировать разрешительную комиссию. В состав комиссии включаются представители Клиента, представители Банка, представители компании-разработчика Системы «iBank2», и при необходимости – независимые эксперты. Выбор членов комиссии осуществляется по согласованию со всеми участниками. При невозможности согласованного выбора последний проводится случайно (по жребию).
7. Стороны передают разрешительной комиссии материалы и документы, подтверждающие факт передачи в Банк Клиентом Электронного документа, авторство, неизменность, подлинность и правильность исполнения Банком Электронного документа, в том числе файлы, записи баз данных, протоколы Соединений (лог-файлы), магнитные и иные носители с записями переговоров или сеансов связи, договоры и соглашения, в соответствии и во исполнение которых сформирован спорный Электронный документ, заявления и другие документы.
8. Разрешительная комиссия на основании изучения представленных Сторонами материалов проводит экспертизу и выносит заключение об обоснованности претензии Клиента большинством голосов.
9. На основании данных технической экспертизы разрешительная комиссия составляет акт.
10. Стороны признают, что акт разрешительной комиссии служит основанием для удовлетворения претензии либо отказе в ее удовлетворении.

Приложение № 5
к Правилам дистанционного банковского обслуживания
физического лица в Системе «iBank2»

РЕКОМЕНДАЦИИ
о порядке действий Клиента в случае выявления хищения денежных средств с использованием Системы «iBank2»

1. В случае выявления хищения денежных средств с использованием Системы «iBank2» немедленно прекратить любые действия с ЭУ в Системе «iBank2», принудительно отключить электропитание и отключить от информационных сетей (если было подключение, например, по USB, Wi-Fi и др.).
2. Обратиться в Банк по телефонам (863) 287-00-58, (812) 456-04-05 (в рабочее время) и после произнесения Блокировочного слова потребовать приостановления исполнения платежа (несанкционированного перевода) и возврата средств, а также приостановления доступа к Системе «iBank2».
3. Обеспечить сохранность (целостность) ЭУ как возможного средства совершения преступления, поместив его в место с ограниченным доступом, обеспечив при этом защиту от вскрытия (стикеры, наклейки, пластилин и т.п.) и по возможности зафиксировать средства контроля целостности фотографированием со всех ракурсов. Если позволяют размеры ЭУ, следует поместить его в непрозрачный пакет (мешок) и опечатать горловину.
4. Обратиться в Банк с письменным Заявлением о приостановлении, отзыве платежа и возврате денежных средств (Приложения № 6) и Уведомлением о блокировании / активации/ создании Учетной записи в Системе «iBank2» (Приложения № 7). Копии Заявления и Уведомления (скан-копии) должны быть направлены в Банк незамедлительно по факсу (863) 287-00-58, (812) 456-04-05 (в рабочее время). Оригиналы Заявления и Уведомления должны быть доставлены в Банк не позднее рабочего дня, следующего за днем обнаружения хищения денежных средств.
5. Предоставить в Банк описание рабочего места Клиента с указанием:
   1) информации о версии операционной системы ЭУ и номера лицензии;
   2) перечня программного обеспечения, используемых на ЭУ (с указанием номеров лицензий);
   3) антивирусного программного обеспечения и способов обеспечения антивирусной защиты;
   4) о выполнении или невыполнении Рекомендаций Банка по мерам безопасности при работе с Системой «bank2» (указанных в Приложении №3).
6. Незамедлительно проинформировать все банки, с которыми Клиент имеет договорные отношения, предусматривающие использование системы интернет-банкинга, о факте хищения денежных средств и обратиться с просьбой о внеплановой замене ключевой информации.
7. В течение 1 (Одного) дня обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств.
8. По согласованию со специальными службами полиции обратиться с письменным заявлением к своему Интернет-провайдеру (рекомендуемая форма Заявления – Приложение № 8 к настоящим Правилам) для получения в электронной форме журналов соединений с Интернет с электронного устройства Клиента или из его локальной вычислительной сети как минимум за три месяца, предшествовавшие факту хищения денежных средств.
9. Не предпринимать никаких действий для самостоятельного или с привлечением сторонних IT-специалистов поиска и удаления компьютерных вирусов, восстановления работоспособности ЭУ, не отправлять ЭУ в сервисные службы ИТ для восстановления работоспособности.
10. Подготовить объяснения о значимых действиях и событиях, в том числе действия с ЭУ, подключенным к Системе «iBank2», предшествовавших факту хищения денежных средств об использовании ЭУ в целях, отличных от осуществления операций в Системе «iBank2», посещаемых сайтах, о странностях при работе ЭУ, перебоях или отказах ЭУ, обращениях в ИТ-службы, в банк плательщика, о сторонних лицах, побывавших в месте расположения ЭУ и т.д.
11. Зафиксировать в протокольной форме значимые действия и события, в том числе действия с ЭУ, подключенным к Системе «iBank2», предшествовавшие факту хищения денежных средств, подготовить объяснения Клиента об использовании ЭУ в целях, отличных от осуществления операций в Системе «iBank2», посещаемых сайтах, о странностях при работе ЭУ, перебоях или отказах ЭУ, обращениях в ИТ-службы, в Банк, о сторонних лицах, побывавших в месте расположения ЭУ и т.д.
12. Оперативно обратиться в суд с исковым заявлением в отношении получателя денежных средств (указав все известные реквизиты получателя) о взыскании неосновательно полученного обогащения и процентов за пользование денежными средствами (глава 60 ГК РФ), а также с ходатайством о принятии судом мер по обеспечению иска в виде ареста денежных средств на счете получателя в сумме неосновательно полученного обогащения. К исковому заявлению необходимо приложить копию заявления о возбуждении уголовного дела либо копию талона КУСП, содержащую отметку правоохранительного органа о его приеме.

Приложение № 6
к Правилам дистанционного банковского обслуживания
физического лица в Системе «iBank2»

Председателю Правления
ООО КБ «РостФинанс»
Прохватилову А.Б.
клиента
Фамилия Имя Отчество,
Дата рождения: «__» _____ _____г.
Документ, удостоверяющий личность:
серия ____ № _____
выдан: _____
дата выдачи: ___ _____ _____ г.
Адрес регистрации: _____

ЗАЯВЛЕНИЕ
о приостановлении, отзыве платежа и возврате денежных средств

«___» _____ 20___ года с моего Счета
№ _____, открытого в ООО КБ «РостФинанс», с использованием Системы «iBank2» были похищены денежные средства, которые, по имеющейся информации, были переведены со следующими реквизитами платежа:
Дата составления документа: _____
Номер документа:_____
Сумма платежа:_____
Наименование плательщика:_____
ИНН плательщика:_____
Номер счета плательщика:_____
Наименование банка плательщика:_____
БИК банка плательщика:_____
Корр.счет банка плательщика:_____
Наименование получателя:_____
ИНН получателя:_____
КПП получателя:_____
Номер счета получателя:_____
Наименование банка получателя:_____
БИК банка получателя:_____
Корр.счет банка получателя:_____
Назначение платежа:
_____
Прошу Вас оказать содействие в приостановлении платежа/ отзыве платежа и возврате денежных средств (нужное подчеркнуть).
Заявление в правоохранительные органы принято в ОВД
_____

_____
_

район, округ, город, субъект федерации и иные идентифицирующие ОВД данные

и зарегистрировано за № _____ в КУСП

Контактные телефоны: _____ моб. _____ дом. _____ раб.

« __ » _____ 20__ г. _____ /**ФИО Клиента /**

(подпись)

Отметка Банка:

Заявление принял: _____ /**ФИО сотрудника**/

(подпись сотрудника)

Приложение № 7
к Правилам дистанционного банковского обслуживания
физического лица в Системе «iBank2»

Руководителю структурного подразделения ООО КБ «РостФинанс»

клиента
Фамилия Имя Отчество,
Дата рождения: «__» _____ _____г.
Документ, удостоверяющий личность:
серия ____ № _____
выдан: _____
дата выдачи: ___ _____ _____ г.
Адрес регистрации: _____

УВЕДОМЛЕНИЕ
о блокировании / активации/ создании Учетной записи в Системе «iBank2»

к правилам на обслуживание физического лица в Системе «iBank2»
№ _____ от «___» _____ 20__ г.

Настоящим уведомляю о своем намерении:

☐ **Блокировать** Учетную запись в Системе «iBank2». Дата и время: «___» _____ 2____г. _____ч. ___мин	☐ **Активировать** Учетную запись, ранее заблокированную по моему распоряжению/ **Создать новую** Учетную запись (нужное подчеркнуть). Дата и время: «___» _____ 2____г. _____ч. ___мин

«__» _____ 20___г. _____ /**ФИО Клиента**/
(подпись)

Отметки Банка:

Заявление принял: _____ /**ФИО сотрудника**/
(подпись сотрудника)

Изменения внесены: «____» _____ 2___г. _____ ч. _____ мин.
(дата и время)

Уполномоченный сотрудник: _____ /**ФИО сотрудника**/
(подпись сотрудника)

Приложение № 8
к Правилам дистанционного банковского обслуживания
физического лица в Системе «iBank2»

_____
должность руководителя

_____
наименование организации

_____
ФИО руководителя

от _____
ФИО Клиента

«_____» _____ _____ г.р.
дата рождения Клиента

_____
Наименование документа, удостоверяющего личность

_____ №_____
серия номер

_____
кем выдан

«_____» _____ _____ г.
дата выдачи

ЗАЯВЛЕНИЕ ИНТЕРНЕТ-ПРОВАЙДЕРУ
о предоставлении журналов соединений (логов)

«____» _____ 20___ года в __: __ по московскому времени со счета _____ по Системе дистанционного банковского обслуживания «iBank2» был осуществлен несанкционированный перевод денежных средств. Компьютер, с которого осуществляется подключение к Системе «iBank2», располагается по адресу _____ и использует IP-адрес ___.___.___.___. Вероятной причиной несанкционированного перевода могло послужить заражение компьютера вредоносным программным обеспечением/ кража логина, пароля и секретных ключей системы «iBank2».

«____» _____ 20__ года между _____ и Вами был заключен договор № _____ на оказание услуг по доступу в сеть Интернет. Для выявления обстоятельств несанкционированного перевода прошу предоставить информацию из журналов (логов) о входящем и исходящем трафике за период с «____» _____ 20___ года по «____» _____ 20___ года с указанием времени соединения, IP и MAC-адресов.

_____ _____ _____
ФИО Клиента подпись расшифровка подписи

«___» _____ 20__

_____
контактные телефоны Клиента

Приложение № 9
к Правилам дистанционного банковского обслуживания
физического лица в Системе «iBank2»

Руководителю структурного подразделения ООО КБ «РостФинанс»

клиента
Фамилия Имя Отчество,
Дата рождения: «__» _____ _____г.
Документ, удостоверяющий личность:
серия ____ № _____
выдан: _____
дата выдачи: ___ _____ _____ г.
Адрес регистрации: _____

ЗАЯВЛЕНИЕ
о расторжении договора на обслуживание физического лица в Системе «iBank2»

Прошу расторгнуть д**оговор на обслуживание физического лица в Системе «iBank2» № ___ от _____ г.** и отключить меня от Системы «iBank2».

«» г. _____ /ФИО Клиента /
(подпись)

Отметки Банка:

Заявление принял: _____ /**ФИО сотрудника**/
(подпись сотрудника)

Клиент отключен: «____» _____ 2___г. _____ ч. _____ мин.
(дата и время)

Уполномоченный сотрудник _____ /**ФИО сотрудника**/
(подпись сотрудника)

Приложение № 10
к Правилам дистанционного банковского обслуживания
физического лица в Системе «iBank2»

Руководителю структурного подразделения
ООО КБ «РостФинанс»

клиента
Фамилия Имя Отчество,
Дата рождения: «__» _____ _____г.
Документ, удостоверяющий личность:
серия ____ № _____
выдан: _____
дата выдачи: ___ _____ _____ г.
Адрес регистрации: _____

ЗАЯВЛЕНИЕ

об изменении контактных данных /отображения счетов
к договору на обслуживание физического лица в Системе «iBank2»
№ ____ от «___» _____ 2___ г.

☐ **Прошу изменить зарегистрированный номер мобильного телефона для получения одноразовых паролей и уведомлений по Системе «iBank2»:**

+7										

☐ **Прошу изменить Блокировочное слово:**

☐ **Прошу предоставить мне доступ к следующим счетам:**

Номер счета	Режим подключения

☐ **Прошу отключить мне доступ к следующим счетам:**

Номер счета	Режим подключения

«__»_____ 20__ г. _____ **/ФИО Клиента/**
(подпись)

Отметки Банка:

Заявление принял: _____ **/ФИО сотрудника/**
(подпись сотрудника)

Изменения внесены: «____» _____ 2___г. _____ ч. _____ мин.
(дата и время)

Уполномоченный сотрудник: _____ **/ФИО сотрудника/**
(подпись сотрудника)

Приложение № 11
к Правилам дистанционного банковского обслуживания
физического лица в Системе «iBank2»

ЗАЯВЛЕНИЕ
об отзыве платежа

Прошу отозвать электронный документ, переданный по Системе «iBank2», со следующими реквизитами платежа:
Дата составления документа: _____
Номер документа:_____
Сумма
платежа:_____
Наименование
плательщика:_____
ИНН
плательщика:_____
Номер счета
плательщика:_____
Наименование банка
плательщика:_____
БИК банка плательщика:_____
Корр.счет банка
плательщика:_____
Наименование
получателя:_____
ИНН
получателя:_____
КПП
получателя:_____
Номер счета
получателя:_____
Наименование банка
получателя:_____
БИК банка получателя:_____
Корр.счет банка получателя:_____
Назначение платежа:
_____

Приложение № 12
к Правилам дистанционного банковского обслуживания
физического лица в Системе «iBank2»

ЛИМИТЫ

на осуществление банковских операций физическими лицами

в Системе «iBank2»

<table>
<tr><th rowspan="2">№ п/п</th><th rowspan="2">Наименование операции</th><th colspan="2">Размер Лимита</th></tr>
<tr><th>В день, руб.</th><th>Одной операции, руб.</th></tr>
<tr><td>1.1.</td><td>Внутрибанковские переводы между своими счетами в валюте Российской Федерации. Переводы платежей в бюджет и во внебюджетные фонды Российской Федерации</td><td rowspan="6">600 000</td><td>Без ограничений</td></tr>
<tr><td>1.2.</td><td>Переводы в валюте Российской Федерации на счета других клиентов – физических[1] и юридических лиц, открытые в Банке и в других кредитных организациях, в т.ч. в режиме «Оплата услуг» (за исключением п.1.3.)</td><td>100 000</td></tr>
<tr><td rowspan="3">1.3.</td><td>Платежи в адрес получателей: Билайн, Мегафон, МТС, Теле 2, иных операторов сотовой связи;</td><td rowspan="3">15 000</td></tr>
<tr><td>Яндекс.Деньги, QIWI, RAPIDA, WebMoney, оплата любых электронных кошельков</td></tr>
<tr><td>Перевод денежных средств с банковской карты Банка на банковскую карту любого российского банка (услуга «Card2Card») [2]</td></tr>
<tr><td>1.4.</td><td>Внутрибанковские переводы на свои счета (в случае, если счет списания и счет зачисления открыты в разных валютах (безналичная конверсия))[3]</td><td>600 000</td></tr>
<tr><td colspan="4">[1] Переводы на счета Банковских карт осуществляются при условии указания лицевого счета Банковской карты и реквизитов Банка – эмитента.</td></tr>
<tr><td colspan="4">[2] Переводы осуществляются при условии указания номера Банковской карты физического лица – получателя перевода.</td></tr>
<tr><td colspan="4">[3] Услуга предоставляется с понедельника по пятницу с 9 часов 00 минут до 16 часов 00 минут МСК</td></tr>
</table>