Утверждены

Приказом Генерального директора АО «Точка»

№ 01 «31» января 2019г.

ПРАВИЛА ДИСТАНЦИОННОГО ОБСЛУЖИВАНИЯ АКЦИОНЕРНОГО ОБЩЕСТВА «ТОЧКА»

Оглавление

1 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Авторизация – подтверждение полномочий (предоставление прав доступа) Клиента, успешно прошедшего Аутентификацию входа, на получение услуг Оператора и/или Банка-партнера посредством Систем ДО на протяжении одного Сеанса связи.

Авторизованный номер – номер мобильного телефона Клиента, предоставленный Клиентом Оператору, и зарегистрированный в Системе ДО. Данные, отправленные на указанный номер телефона, считаются безусловно полученными надлежащим пользователем.

Активация – создание Цифрового кода/Touch ID кода для получения доступа к ДО, после первой успешной Аутентификации входа.

Аутентификация – удостоверение правомочности обращения Клиента к Оператору для совершения действий в порядке, предусмотренном настоящими Правилами.

Аутентификация операции – процедура проверки принадлежности Клиенту полученного Оператором посредством Системы ДО Электронного документа, выполняемая во время Сеанса связи с использованием ЭП.

Аутентификация входа – процедура проверки соответствия предъявленных Базовых аутентификационных данных и Одноразового ключа (при наличии), либо Цифрового кода/Touch ID, выполняемая перед установлением Сеанса связи. Без успешной Аутентификации входа Сеанс связи не устанавливается.

Базовые аутентификационные данные – присвоенный Оператором Клиенту Логин и установленный Клиентом самостоятельно Пароль, используемые для целей Аутентификации входа.

Банк-партнер – банк-участник информационной системы.

Банками-партнерами являются:

- Публичное акционерное общество Банк «Финансовая Корпорация Открытие», Генеральная лицензия ЦБ РФ № 2209 от 24.11.2014, ОГРН 1027739019208;

- КИВИ Банк (акционерное общество), Лицензия на осуществление банковских операций №2241 от 22.01.2015, ОГРН 1027739328440.

Оператор вправе в любое время вносить изменения в указанный список Банков-партнеров, в случае присоединения к настоящим Правилам новых Банков-партнеров, либо их исключения.

Банковская карта (Карта) – расчетная карта, эмитированная Банком-партнером.

Виджет – это дополнение к Мобильному приложению для Портативных устройств, требующее установки, которое позволяет Клиенту получать информацию непосредственно из Мобильного приложения в режиме реального времени.

Владелец ЭП – физическое лицо, имеющее Базовые аутентификационные данные и присоединившееся к настоящим Правилам.

Договор дистанционного обслуживания (Договор) – совокупность настоящих Правил и подписанного Клиентом Заявления о присоединении к настоящим Правилам по форме соответствующих приложений к настоящим Правилам.

Договор комплексного банковского обслуживания (ДКБО) – договор, заключенный с Клиентом путем присоединения Клиента к Правилам банковского обслуживания посредством использования ЭП в Системе ДО.

Дополнительные аутентификационные данные – связанные с Базовыми аутентификационными данными личные идентификаторы пользователя (логин и пароль) в ЕСИА. Применение Дополнительных аутентификационных данных является опциональным и остается на усмотрение Клиента. В процессе аутентификации входа с использованием сервиса ЕСИА вместо логина и пароля аккаунта в ЕСИА, проверке могут подвергаться идентификаторы активной сессии в ЕСИА и соответствующие ей данные ограниченного доступа (т.н. cookie) на компьютере Клиента.

Дистанционное обслуживание (ДО)- способ предоставления услуг посредством телекоммуникационной сети «Интернет».

Единая система идентификации и аутентификации (ЕСИА) — информационная система в Российской Федерации, обеспечивающая санкционированный доступ участников информационного взаимодействия (граждан-заявителей и должностных лиц органов исполнительной власти) к информации, содержащейся в государственных информационных системах и иных информационных системах. Условия использования ЕСИА доступны на сайте в сети Интернет: https://esia.gosuslugi.ru/registration/policiesTerms.xhtml.

Заявление о присоединении - заявление по форме соответствующего Приложения к настоящим Правилам о присоединении Клиента к настоящим Правилам в целях заключения Договора дистанционного обслуживания.

Идентификационные данные – сведения, предназначенные для Аутентификации Клиента при обращении к Оператору.

Идентификатор Клиента – уникальная взаимно-однозначно связанная с Базовыми аутентификационными данными последовательность символов, используемая для обмена данными во время Сеансов связи в Системе «Точка».

Клиент – Владелец ЭП. После присоединения Владельцем ЭП к ПБО, в качестве Уполномоченного лица, и при использовании функционала распоряжения Счетом, иных услуг Банков-партнеров термин «Клиент» употребляется в соответствии с определением соответствующих Правил банковского обслуживания Банка-партнера.

Ключ ЭП - уникальная последовательность символов, состоящая из Базовых аутентификационных данных предназначенная для создания ЭП. Для Мобильного приложения Ключом ЭП является Цифровой код или Touch ID. Для Личного кабинета Ключом ЭП является Пароль.

Код OTP-токена – Код авторизации, считываемый Клиентом с экрана OTP-токена.

Колл-центр - сервис Оператора, позволяющий Клиенту после его успешной Аутентификации посредством телефонного канала связи при участии сотрудника Оператора дистанционно давать Оператору указания на совершение действий во исполнение Договора и/или ДКБО и получать справочную информацию в порядке и на условиях, предусмотренных Договором и/или ДКБО.

Компрометация Ключа ЭП - ситуация при которой есть достаточные основания полагать, что доверие к тому, что используемый Ключ ЭП обеспечивают безопасность информации, утрачено. К событиям, связанным с компрометацией Ключа ЭП относятся, включая, но, не ограничиваясь, следующие:

- утрата ключевых носителей;
- утрата ключевых носителей с последующим обнаружением;
- нарушение правил хранения и уничтожения секретного ключа;
- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи; о случаи, когда нельзя достоверно установить, что произошло с носителями, содержащими ключевую информацию (в том числе случаи, когда носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

Личный кабинет - Система ДО, обеспечивающая формирование, передачу, регистрацию ЭД (в т.ч. распоряжений Клиента о переводе денежных средств), передачу и получение информации при исполнении Договора, ДКБО, посредством дистанционного взаимодействия, в порядке, определенном настоящими Правилами. Функционал дистанционного доступа Клиента к Счету становится доступен в Личном кабинете после заключения Клиентом ДКБО.

Логин – уникальная взаимно-однозначно связанная с Базовыми аутентификационными данными последовательность символов, предоставляемая Оператором Клиенту. Логин может быть изменен Клиентом самостоятельно неограниченное количество раз.

Мессенджер - разновидность Открытого канала связи, позволяющего обмениваться сообщениями с Оператором в режиме реального времени. Включает в себя, но не ограничивается, следующими приложениями для Портативных устройств и web-интерфейсами:

• Viber (https://www.viber.com/);

• Telegram (https://telegram.org/).

Мобильное приложение (Система «Точка») – приложение для портативных устройств, работающих под управлением операционной системы iOS или Android, обеспечивающее формирование, передачу, регистрацию ЭД (в т.ч. распоряжений Клиента о переводе денежных средств), передачу и получение информации при исполнении Договора, ДКБО посредством дистанционного взаимодействия, в порядке, определенном настоящими Правилами.

Одноразовый ключ – набор цифр и/или символов, отправленных Клиенту в СМС-сообщении, сгенерированный Клиентом на OTP-токене посредством нажатия кнопки на устройстве. Время действительности Одноразового ключа является ограниченным, и определяется Оператором. Применение Одноразового ключа на операцию является однократным. Одноразовый ключ служит для подтверждения принадлежности Сессионного ключа Клиенту.

Онлайн-консультант (Чат) – это сервис для предоставления консультаций для авторизованных пользователей систем ДО в режиме реального времени.

Открытый канал связи – это такой канал, передачи информации в которых осуществляется без ее дополнительной защиты (шифрование канала и\или самой информации) от несанкционированного доступа и изменения со стороны третьих лиц (например - Интернет, электронная почта и т.д.).
OTP-токен - техническое устройство в виде брелока, которое генерирует коды авторизации при нажатии Клиентом на кнопку, расположенную на устройстве.

Оператор - Акционерное общество «Точка», ИНН 9705120864, место нахождения: 109240, г. Москва, ул. Верхняя Радищевская, д.2/1, строение 5, пом.1, эт.3, ком.4, являющееся организатором ИС.

Операция по Счету (Операция) - принятие и зачисление на Счет, перечисление и выдача со Счета денежных средств.

Пароль - уникальная последовательность буквенных, числовых и иных символов, известная только Владельцу ЭП, соответствующая присвоенному ему Логину и использующаяся для Аутентификации Клиента в Системе ДО.

Подтверждение подлинности ЭД - положительный результат проверки ЭП в ЭД.

Портативное устройство – смартфоны, планшетные компьютеры, работающие под управлением операционной системы iOS 8 или Android 4.1 и выше.

Правила банковского обслуживания (ПБО) – Правила банковского обслуживания Клиентов – участников информационной системы «Точка» - условия обслуживания

Клиентов в Банке-партнере, на которых заключается Договор комплексного банковского обслуживания.

Правила дистанционного обслуживания (Правила) – Правила дистанционного обслуживания АО «Точка» – условия обслуживания Клиентов, на которых заключается Договор дистанционного обслуживания.

Проверка ЭП – процедура проверки корректности ЭП под ЭД.

Разрешительная комиссия - комиссия, создаваемая Сторонами для разрешения разногласий, возникающих при обмене ЭД.

Сайт Оператора – официальный сайт Оператора в сети Интернет www.tochka.com.

Сеанс связи – период времени, в течение которого Клиент авторизован на работу в Системе ДО, обеспечивающий непрерывное взаимодействие Оператора и Клиента. Для начала Сеанса связи необходимо успешно пройти Аутентификацию входа.

Сервис «Робопин» - система, обеспечивающая посредством телефонной связи возможность установить/изменить ПИН-код к Банковской карте.

Сессионный ключ – уникальная последовательность символов, предназначенная для проверки авторства ЭД, направляемых Клиентом в рамках Сеанса связи. Сессионный ключ формируется после успешного прохождения Аутентификации входа на основании Цифрового кода/Touch ID кода Клиента, Базовых аутентификационных данных. С помощью Сессионного ключа осуществляется проверка подлинности ЭД, направляемых Клиентом в рамках Сеанса связи. По своей сути является простой электронной подписью.

Система дистанционного обслуживания (Система ДО) – программно-технический комплекс, позволяющий Участникам информационного взаимодействия посредством использования ЭП, совершать определенные Правилами действия. Системами ДО является: Личный кабинет, Мобильное приложение.

Стороны – Участники информационного взаимодействия – Оператор, Банк-партнер, Клиент.

Средство аутентификации – Логин и Пароль, Одноразовые ключи, и иные средства, используемые с целью Аутентификации Клиента.

Схема Авторизации - схема получения Одноразовых ключей (СМС-кодов, OTP-токена и других), которую Клиент выбирает самостоятельно, заполнив и подписав заявление на смену Схемы Авторизации в системе ДО.

Счет –счета в рублях РФ, в иностранной валюте, открытые Клиентами в Филиале Банка-партнера в соответствии с Правилами банковского обслуживания.

Тарифы Оператора - перечень ставок, условий и порядок оплаты услуг, оказываемых Оператором Клиентам.

Тарифы Филиала – сведенный в единый документ перечень ставок, условий и порядок оплаты услуг, оказываемых Клиентам в Филиале.

Технология 3-D Secure - защищенный протокол авторизации Клиента, который добавляет дополнительный шаг авторизации при оплате товаров, услуг в сети Интернет с использованием Банковской карты, путем ввода SecureCode.

Уполномоченное лицо – лицо (включая единоличный исполнительный орган), действующее от имени и в интересах Клиента, полномочия которого основаны на уставе, доверенности или договоре.

Уточнение платежа по телефону - услуга, позволяющая Клиенту обратиться в Колл-центр Оператора посредством телефонного канала связи, с целью уточнения реквизитов ЭД, ранее направленного в Банк-партнер посредством Систем ДО.

Участники информационной системы - Оператор, Банк-партнер, Клиент.

Филиал – филиал Банка-партнера, где Клиент непосредственно получает банковские услуги, а именно:

• Филиал Точка Публичного акционерного общества Банка «Финансовая Корпорация Открытие» или

• Филиал Точка Банк КИВИ Банк (акционерное общество).

Хэш-сумма - результат обработки файла хэш-функцией.

Хэш-функция – однонаправленное отображение (свертка) содержимого файла произвольного размера в блок данных фиксированного размера, обладающее заданными математическими свойствами; используется при формировании и проверке ЭД для контроля целостности передаваемых вместе с ЭД файлов.

Цифровой код – комбинация из четырех цифр, устанавливаемая Клиентом (и известная только Клиенту) в Мобильном приложении при Активации. Цифровой код Клиента обеспечивает однозначную Аутентификацию входа.

Электронный документ (ЭД) - документ, информация в котором представлена в электронной форме.

Электронная подпись (ЭП) – 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. В настоящих Правилах используется простая ЭП, используемая в Системах ДО.

Bot (Бот) – специальная программа, выполняющая автоматически и/или по заданному расписанию какие-либо действия через те же интерфейсы, что и обычный пользователь. При обсуждении компьютерных программ термин употребляется в основном в применении к Интернету.

Facebook (Фейсбук) – социальная сеть (платформа, онлайн-сервис и веб-сайт, предназначенные для построения, отражения и организации социальных взаимоотношений), доступная в сети Интернет, а также одноименное мобильное приложение для Портативных устройств. Позволяет пользователям обмениваться текстовыми сообщениями. Приложение доступно для установки на Портативное устройство в официальных репозиториях (хранилищах) мобильных приложений app store, play market и прочих под именем Facebook (разработка Facebook).

Facebook_bot – специальная программа для Facebook, позволяющая по соответствующему запросу пользователей через Facebook автоматически и/или по заданному расписанию

выполнять какие-либо действия/операции в целях выполнения запросов пользователей. Запросы пользователей, отправленные Боту, обрабатываются Оператором.

Push-уведомление – сообщение, передаваемое Оператором Клиенту на Портативное устройство Клиента посредством Мобильного приложения.

Telegram – мобильное приложение для Портативных устройств, позволяющее пользователям обмениваться текстовыми сообщениями и файлами различных форматов. Приложение доступно для установки на Портативное устройство в официальных репозиториях (хранилищах) мобильных приложений app store, play market и прочих под именем Telegram Messenger (разработка Telegram LLC).

Touch ID – технология аутентификации с помощью сканера отпечатков пальцев, встроенная в Портативное устройство Клиента, инициируемая Мобильным приложением, посредством обращения к данной процедуре в устройстве для выполнения аутентификации пользователя. Для целей Правил термин Touch ID распространяется не только на продукцию компании Apple, но и на иные платформы, на базе которых работают Портативные устройства.

Touch ID код – результат проверки Touch ID.

3D Touch – технология, встроенная в дисплей Портативного устройства компании Apple (поддерживающего данную технологию), которая распознает силу нажатия, на различных уровнях натиска. Технология позволяет Клиенту получать информацию непосредственно из Мобильного приложения в режиме реального времени.

Понятия, специально не определенные в настоящих Правилах, применяются в значениях, установленных действующим законодательством РФ, и в соответствии с их буквальным смыслом и толкованием, исходя из контекста фразы в Правилах.

2 ПОРЯДОК ЗАКЛЮЧЕНИЯ И ИЗМЕНЕНИЯ ДОГОВОРА, ПРАВИЛ. ОБЩИЕ ПОЛОЖЕНИЯ

2.1 Настоящие Правила являются документом Оператора, устанавливающим порядок заключения и исполнения Договора, порядок оказания услуг в Системах ДО, перечень услуг и сервисов, предоставляемых в Системах ДО, а также иные условия, необходимые для функционирования информационной системы.

2.2 Совокупность настоящих Правил и Заявление Клиента о присоединении к Правилам являются документами, составляющими заключенный между Сторонами Договор дистанционного обслуживания.

2.3 Оператор вправе принять от Клиента Заявление о присоединении к Правилам по формам, отличающимся от форм приложений к настоящим Правилам.

2.4 Заключение Договора осуществляется в соответствии со статьей 428 Гражданского кодекса РФ путем присоединения к Правилам. Стороны вправе подписать Заявление о присоединении на бумажном носителе.

2.5 В целях заключения Договора Клиент и Оператор совершают следующие действия:

2.5.1 Оператор по волеизъявлению Клиента путём направления на номер мобильного телефона Клиента, который Клиент предоставил Оператору, выдает Клиенту Логин. Клиент самостоятельно устанавливает Пароль.

2.5.2 Клиент в присутствии сотрудника Оператора, используя Логин и Пароль, заходит в Систему ДО, где, следуя экранным формам, заносит свои данные в электронную форму Заявления о присоединении, тем самым совершая конклюдентные действия, направленные на заключение Договора, подтверждая действительность предоставленных сведений и свое согласие с текстом Заявления о присоединении и Правил[1].

2.5.3 Оператор отправляет Клиенту СМС-сообщение с Одноразовым ключом и номером ID документа.

2.5.4 Клиент сверяет номер ID документа, полученный в СМС-сообщении с номером ID документа, указанным в Заявлении о присоединении. При совпадении указанных номеров, Клиент вводит в экранной форме Одноразовый ключ, полученный от Оператора, подтверждая свое волеизъявление на заключение Договора.

2.5.5 Моментом присоединения к Правилам и моментом заключения Договора с Клиентом, за исключением случаев, предусмотренных настоящими Правилами, является момент размещения Оператором в Системе ДО уведомления о заключении Договора.

2.6 После заключения Договора Стороны вправе приступить к обмену ЭД посредством ЭП в Системе ДО в пределах доступного функционала.

2.7 Клиенты, присоединившиеся к Правилам банковского обслуживания Банка-партнера до 01.02.2019г., автоматически становятся участниками информационной системы и обслуживаются в соответствии с настоящими Правилами и Правилами банковского обслуживания в редакции, предусматривающей привлечение Оператора для оказания услуг ДО посредством Систем ДО. Совершая любую операцию посредством Системы ДО после 31.01.2019г., Клиент подтверждает присоединение к настоящим Правилам, моментом присоединения к Правилам и моментом заключения Договора между Оператором и Клиентом является момент совершения любой операции, любого действия в Системе ДО.

2.8 Предоставление услуг Клиенту осуществляется только посредством Систем ДО.

2.9 Настоящие Правила является неотъемлемой частью Договора дистанционного обслуживания и определяют условия обмена ЭД с использованием ЭП между Оператором, Банками-партерами и Клиентом. Дистанционное обслуживание осуществляется с момента заключения Договора и до момента расторжения Договора или прекращения Дистанционного обслуживания в случаях, предусмотренных настоящими Правилами.

2.10 Стороны могут заключить двухстороннее соглашение, изменяющее и/или дополняющее/исключающее применение отдельных положений Правил и/или Тарифов. В этом случае Правила действуют в части, не противоречащей условиям указанного соглашения.

2.11 Заключение соглашений об изменении или дополнении Договора, иных договоров, предусмотренных Правилами может осуществляться следующими, согласованными Сторонами способами для заключения сделок в письменной форме:

[1] Договор считается заключенным, когда из поведения Сторон явствует их воля на заключение Договора (пункт 2 статьи 158, пункт 3 статьи 432 ГК РФ).

• составление Сторонами одного документа, подписанного Сторонами;

• обмен документами по Системе ДО. В этом случае не требуется дополнительных доказательств того, что документ исходит от Стороны по Договору. Документы в электронной форме, подписанные ЭП, полностью приравниваются по юридической силе к документам на бумажном носителе, подписанным собственноручными подписями Уполномоченных лиц Сторон Договора. Изменения в Договор считаются заключенными с момента направления Оператором акцепта Клиенту по Системе ДО о согласии Оператора изменить условия Договора в редакции, предложенной Клиентом;

• путем изменения Правил и/или Тарифов в порядке, предусмотренном настоящими Правилами.

2.12 Изменение и расторжение Договора возможны по соглашению Сторон, в одностороннем порядке по основаниям и в порядке, определенном в законодательстве РФ и настоящими Правилами.

2.13 Соглашение о расторжении Договора совершается в той же форме, что и Договор, путем:

- составления Сторонами одного документа, подписанного Сторонами в системе ДО;

- направления Клиентом Оператору заявления о расторжении Договора.

2.14 Внесение изменений и дополнений в настоящие Правила и/или Тарифы производится Оператором в одностороннем порядке.

2.15 Для вступления в силу изменений и дополнений в Правила, вносимых Оператором по собственной инициативе, Оператор информирует Клиента о таких изменениях и дополнениях не позднее, чем за 5 (пять) календарных дней до даты введения в действие изменений.

2.16 Оператор с целью ознакомления Клиентов с настоящими Правилами, изменениями, дополнениями к ним, Тарифами, изменениями и дополнениями к ним доводит информацию до Клиентов одним или несколькими способами:

• размещение новой редакции Правил и/или Тарифов на сайте Оператора (Основной способ ознакомления);

• оповещение Клиентов посредством Системы ДО;

• направление Клиентам СМС-сообщений/Push-уведомлений.

2.17 Датой ознакомления Клиента с новой редакцией Правил и/или Тарифов и изменений и/или дополнений к ним считается дата размещения Оператором информации об изменениях и/или дополнениях и текста Правил и/или Тарифов в новой редакции на сайте Оператора.

2.18 Уведомление Оператором Клиента не требует получения от Клиента доказательств получения такого уведомления. Клиент не вправе ссылаться на незнание информации об изменении и/или дополнении Правил и/или Тарифов в случае неисполнения или ненадлежащего исполнения обязательств по Договору.

2.19 Все изменения и дополнения, вносимые Оператором в Правила и/или Тарифы, вступают в силу, начиная со дня, следующего за днем истечения срока, указанного в п. 2.15 настоящих Правил.

2.20 Клиент вправе не согласиться с изменениями, внесенными Оператором, направив заявление в порядке, определенном настоящими Правилами. В случае неполучения Оператором указанного заявления о расторжении Договора до даты ввода в действие изменений в Правила Стороны считают это согласием Клиента с указанными изменениями. При этом Клиент не может расторгнуть Договор при наличии действующего ДКБО с Банком-партнером.

2.21 Оператор не несет ответственности, если информация об изменении и/или дополнении Правил и/или Тарифов, опубликованная в порядке и в сроки, установленные настоящими Правилами, не была получена Клиентом, Клиент с ней не ознакомился и не принял к сведению.

3 ПОРЯДОК ДИСТАНЦИОННОГО ОБСЛУЖИВАНИЯ

3.1 Настоящий порядок определяет условия обмена ЭД с использованием ЭП между Сторонами Договора. ДО осуществляется с момента заключения Договора до момента расторжения Договора или прекращения ДО в случаях, предусмотренных настоящими Правилами.

3.2 Стороны договорились об использовании между ними ЭП в Системах ДО для:

- заключения и исполнения любых гражданско-правовых сделок, если специальный порядок заключения, изменения, расторжения не указан в иных разделах настоящих Правил и/или Правил банковского обслуживания;
- после заключения ДКБО совершения Клиентом любых банковских операций в соответствии с действующим законодательством;
- оформления доверенности на представительство перед Участниками информационного взаимодействия, в т.ч. на право распоряжения Счетом, совершение иных действий, необходимых для открытия/закрытия и обслуживания Счетов, Банковских карт;
- передачи любых заявлений и сообщений;
- обмена любой информацией и документами;
- формирования неограниченного количества ЭП любых видов в т.ч. для подписания расчетных и иных документов в отношении любых Счетов, в том числе и вновь открываемых;
- достижения договоренностей об использовании новых ЭП любого вида;
- заключения сделок с аккредитованным удостоверяющим центром и получения квалифицированной ЭП;
- совершения иных юридически значимых действий, направленных на исполнение обязательств, установление, изменение или прекращение правоотношений Сторон.

3.3 Стороны признают ЭД, подписанные ЭП равнозначными документам на бумажных носителях, подписанным собственноручной подписью, а также общий порядок и условия использования ЭП.

3.4 В рамках настоящих Правил Стороны признают легитимность Средств аутентификации Клиентов, используемых ими после 31.01.2019г., но полученных в результате присоединения к Правилам банковского обслуживания Банка-партнера до 01.02.2019г. Взаимодействие Сторон посредством таких Средств Аутентификации с 01.02.2019г. регламентируется настоящими Правилами.

3.5 Стороны договариваются об использовании между ними ЭП в Системах ДО в порядке, предусмотренном настоящими Правилами.

3.6 ЭД порождает обязательства Сторон, если передающей стороной он надлежащим образом оформлен, заверен ЭП и передан, а принимающей стороной получен, проверен и принят.

3.7 ЭД Клиента, созданный с использованием Систем ДО и подписанный ЭП, переданный по согласованным Системам ДО и полученный Оператором, является документом, имеющим юридическую силу, равную аналогичным документам, надлежащим образом, оформленным на бумажных носителях, подписанным собственноручной подписью Уполномоченного лица и заверенным печатью Клиента, если наличие печати на документе необходимо в соответствии с требованиями действующего законодательства РФ.

3.8 Действия, совершенные Сторонами, а также сделки, заключенные между Сторонами посредством ЭП, не могут быть оспорены только на том основании, что эти действия не подтверждаются документами, составленными на бумажных носителях.

3.9 В случае передачи Клиентом Оператору ЭД, подписанного ЭП, с вложениями, вложения считаются также подписанными ЭП и являются эквивалентными подобным документам, составленным на бумажных носителях и влекут аналогичные документам, составленным на бумажном носителе, права и обязанности Сторон.

3.10 Оператор не несет ответственности в случае, если информация о Счетах Клиента, сведения о Клиенте и/или операциях по Счету/Счетам Клиента станет известной третьим лицам в результате прослушивания или перехвата каналов доступа к сети Интернет таких как WiFi во время использования этих каналов Клиентом в режиме ДО.

3.11 Стороны признают в качестве единой шкалы времени при работе в Системах ДО - Московское поясное время. Контрольным является время системных часов аппаратных средств Оператора.

3.12 ЭД считается переданным Клиентом и полученным Оператором если Система ДО подтвердила передачу, присвоила распоряжению регистрационный номер и изменила статус документа на соответствующий в Системе ДО. В случае если по каким-либо причинам (разрыв связи и т.п.) Клиент не получил подтверждения о получении и регистрации ЭД, ответственность за установление окончательного результата передачи ЭД лежит на Клиенте.

3.13 ЭД считается переданным Клиентом, если выполнены все этапы нижеследующей процедуры передачи ЭД:

- Аутентификация входа Клиента прошла успешно;
- Клиент ввел/сообщил содержание ЭД и его параметры;
- Клиент подтвердил правильность ввода ЭД и его параметров.

3.14 Считается, что Клиент отказался от передачи ЭД, если он не подтвердил правильность ввода ЭД и его параметров.

3.15 При использовании ЭП при обмене ЭД Стороны признают, что:

- недопустимо внесение Клиентом изменений в ЭД после его подписания ЭП;
- Клиент несет ответственность за сохранность Средств аутентификации и за действия своего персонала при обмене ЭД;
- при возникновении спора о соблюдении правил обмена ЭД эталоном является журнал обмена ЭД и журнал регистрации блокировок доступа к Системе ДО, хранящиеся на сервере Оператора.

3.16 Для создания ЭП, подписания ЭД и проверки ЭП Стороны используют средства ЭП, согласно принятым рекомендациям Оператора, и признают их достаточными для подтверждения подлинности ЭД, подписанных ЭП.

3.17 В случае необходимости передачи Оператору файлов, в качестве приложения к ЭД Клиента, содержащих необходимую дополнительную информацию для надлежащего исполнения Оператором и/или Банком-партнером ЭД Клиента, с помощью Хэш-функции создается Хэш-сумма для каждого приложенного файла. Хэш-сумма каждого файла указывается в ЭД Клиента, подписанном ЭП.

3.18 При возникновении разногласий и споров относительно неизменности файла, переданного Клиентом и полученного Оператором совместно с ЭД, для проверки неизменности используется полученная с помощью хэш-функции Хэш-сумма файла.

3.19 Смена Ключа ЭП, Авторизованного номера, OTP-токена производится в случае их компрометации, а также в иных случаях, предусмотренных Правилами, ПБО.

3.20 Смена Ключа ЭП и средств ЭП может быть произведена только Владельцем ЭП.

3.21 После ввода в действие новых Ключей ЭП или средств ЭП недействительные (старые) Ключи ЭП и Средства ЭП уничтожаются.

3.22 ЭД Клиентов принимаются Оператором круглосуточно, и выполняются Банком-партнером в рабочие дни в соответствии со сроками выполнения распоряжений Клиентов, установленными регламентом проведения операций Банка-партнера.

3.23 В случае отказа Банка-партнера от выполнения ЭД, переданного Клиентом и зарегистрированного Оператором, Оператор оповещает Клиента о причинах такого отказа по Системе ДО.

3.24 Клиент понимает и соглашается с тем, что использование Клиентом Систем ДО возможно лишь на условиях «как есть», т.е. согласно предоставленному Оператором в любой момент в течение срока действия Договора комплексу функционала, информационного наполнения, интерфейса, дизайна, иных составляющих и условий использования Систем ДО. Клиент выражает свое согласие с предоставленным Оператором в любой момент в течение срока действия Договора комплексом функционала, информационного наполнения, интерфейса, дизайна, иных составляющих и условий использования Систем ДО, путем предоставления Оператору надлежащим образом оформленного и подписанного Клиентом Заявления о присоединении к Правилам. Изменение порядка работы, в том числе интерфейса, дизайна, информационного

наполнения, функционала и любых составляющих Системы ДО по волеизъявлению Клиента технически невозможно, что не является ненадлежащим исполнением Оператором Договора и нарушением прав и законных интересов Клиента. Отзыв Клиентом согласия на обработку персональных данных также не является основанием для внесения Оператором каких-либо изменений в порядок работы Систем ДО, поскольку обработка Оператором персональных данных Клиента в рамках функционирования Систем ДО связана исключительно с исполнением условий Договора.

4 ПРАВА И ОБЯЗАННОСТИ СТОРОН

4.1 Оператор обязуется:

4.1.1 Предоставлять Клиенту услуги по Системе ДО с даты заключения Договора.

4.1.2 Принимать и передавать на исполнение в Банк-партнер полученные по Системе ДО, ЭД, оформленные и подписанные в соответствии с настоящими Правилами.

4.1.3 Предоставить Клиенту возможность получения актуальной и достоверной информации о переданных Клиентом ЭД, операциях по его Счетам, состоянии его Счетов и иную информацию в порядке, предусмотренном настоящими Правилами.

4.1.4 Консультировать Клиента по вопросам обслуживания в Системе ДО.

4.1.5 Принимать меры по защите от несанкционированного доступа к Системам ДО и сохранять конфиденциальность информации по Счетам Клиента.

4.1.6 Сообщать Клиенту об обнаружении попытки несанкционированного доступа к Системе ДО, если это затрагивало операции Клиента.

4.1.7 Принять меры для предотвращения несанкционированного доступа третьих лиц к конфиденциальной информации, составляющей банковскую и коммерческую тайну. Указанная информация может быть предоставлена третьим лицам в порядке, установленном действующим законодательством Российской Федерации.

4.1.8 Размещать в официальных онлайн-магазинах мобильных приложений (AppStore и Play Market) приложения для Портативных устройств.

4.2 Оператор вправе:

4.2.1 В одностороннем порядке изменять перечень услуг, предоставляемых по Системам ДО, по своему усмотрению, разместив соответствующую информацию об услуге и способах ее получения в системе ДО.

4.2.2 Приостановить, ограничить, прекратить или возобновить обслуживание в Системах ДО, а также отказать в исполнении ЭД в случаях и порядке, предусмотренных настоящими Правилами и/или ПБО.

4.2.3 Затребовать от Клиента в любой момент в случае необходимости предоставления документа на бумажном носителе, эквивалентного по смыслу и содержанию переданному Клиентом ЭД, оформленного в соответствии с требованиями действующего законодательства РФ.

4.2.4 Вводить дополнительные способы Аутентификации Клиента.

4.2.5 Вводить ограничения на использование Клиентом Средств аутентификации и аналогов собственноручной подписи.

4.2.6 Заблокировать Средства аутентификации в случае возникновения подозрений о возможной утери, утраты Средств аутентификации, либо доступа к ним третьих лиц.

4.2.7 Прекратить регистрацию ЭД Клиента при неоплате Клиентом комиссий, предусмотренных Тарифами Оператора и/или Банка-партнера.

4.3 Клиент обязуется:

4.3.1 Для использования систем ДО выполнить следующие действия:

• Самостоятельно обеспечить наличие необходимых и достаточных аппаратных, системных, сетевых и телекоммуникационных средств для организации ДО, согласно рекомендациям Оператора, предусмотренным в настоящих Правилах;

• Принять все организационные и технические меры безопасности для предотвращения несанкционированного доступа неуполномоченных лиц к обмену дистанционными распоряжениями;

4.3.2 Соблюдать технические требования к компьютерному и программному обеспечению, определенные в настоящих Правилах и размещенные на сайте www.tochka.com.

4.3.3 Осуществлять ввод документов (и осуществлять контроль введенной информации) в электронном виде, соблюдая порядок подготовки документов, обеспечивая заполнение форм в соответствии с настоящими Правилами.

4.3.4 Соблюдать конфиденциальность информации, касающейся Средств аутентификации, используемых в Системе ДО. Немедленно информировать Оператора об обстоятельствах, которые делают возможным создание ЭД и их передачу посредством Системы ДО лицами, не имеющими соответствующих полномочий, а также обо всех случаях повреждения программно-технических средств Системы ДО, в том числе несанкционированного доступа в Систему ДО.

4.3.5 Принять все риски, связанные с получением третьими лицами сведений о движении денежных средств и остатков на Счете в случае утраты/кражи мобильного телефона, используемого для работы в Системе ДО, либо передачи его третьим лицам, а также по причине утраты/разглашения Клиентом Средств аутентификации.

4.3.6 Соблюдать конфиденциальность информации, касающейся Системы ДО, не разглашать третьим лицам особенности функционирования Системы ДО.

4.3.7 Хранить Средства аутентификации в надежном месте, исключающем доступ к нему неуполномоченных лиц и повреждение материального носителя Ключа ЭП. В случае утери Средств аутентификации незамедлительно уведомить Оператора о данном факте. В противном случае Клиент несет риск неблагоприятных последствий от использования Ключа ЭП неуполномоченными лицами, в том числе риск проведения платежей неуполномоченными лицами.

4.3.8 При осуществлении обмена ЭД:

• соблюдать регламент обмена ЭД;

• информировать Оператора о неисправностях в работе Системы ДО и по запросам Оператора письменно подтверждать наличие этих событий с подробным указанием обстоятельств, при которых они возникли;

• использовать полученные от Оператора программно-технические средства только для целей осуществления ДО в рамках настоящего Договора, не передавать без письменного согласия Оператора данные средства третьим лицам;

• не производить модификацию программных средств, не совершать относительно указанных программно-технических средств других действий, нарушающих действующее законодательство РФ;

• в случае использования Одноразового ключа, полученного посредством СМС- сообщения / Push-уведомления, содержащего параметры перевода, осуществлять проверку Одноразового ключа путем сравнения отправленного в СМС-сообщении /Push-уведомлении Одноразового ключа, сгенерированного в Системе ДО по запросу Клиента, с Одноразовым ключом, введенным Клиентом.

• в случае использования Одноразового ключа, полученного посредством СМС-сообщения/ Push-уведомления, содержащего параметры перевода, осуществлять предварительную сверку реквизитов перевода в СМС-сообщении с данными, введенными в Системе ДО перед совершением перевода;

• не совершать действий, способных привести к нарушению целостности Системы ДО, а также незамедлительно сообщать Оператору о ставших известными попытках третьих лиц совершить действия, способные привести к нарушению целостности Системы ДО;

• соблюдать порядок разрешения споров, установленный настоящими Правилами;

• при Компрометации Ключа ЭП незамедлительно произвести действия по приостановлению обмена ЭД, непосредственно сообщив об этом Оператору по Системам ДО либо по телефону +7-800-2000-024 (служба технической поддержки).

4.3.9 В случае компрометации Ключа ЭП, его утраты, хищения, выбытия из владения Клиента по другому основанию или обнаружения факта совершения несанкционированных операций с использованием Ключа ЭП Клиент обязан незамедлительно, но не позднее дня, следующего за днем получения информации о совершенной операции или установления факта компрометации/утраты/хищения/выбытия по другому основанию Ключа ЭП совершить следующие действия:

• уведомить Оператора по Системе ДО об отмене действия соответствующего Ключа ЭП;

• уведомить Оператора об обнаружении факта совершения несанкционированной операции. Текст уведомления должен содержать следующие данные:

1) ФИО и/или наименование Клиента;

2) данные документа, удостоверяющего личность владельца Счета/Уполномоченного лица Клиента;

3) дату компрометации/хищения/утраты/выбытия из владения Клиента Ключа ЭП;

4) даты обнаружения и совершения, сумму несанкционированной операции;

5) данные получателя.

4.4 Клиент вправе:

4.4.1 Использовать Системы ДО в порядке и на условиях, оговоренными настоящими Правилами.

4.4.2 По заявлению приостановить, ограничить, прекратить или возобновить обслуживание в Системе ДО в случаях и порядке, предусмотренных настоящими Правилами.

4.4.3 Отменить действие Ключа ЭП, направив Оператору уведомление об отмене действия Ключа ЭП. Ключ ЭП считается отмененным с момента подтверждения Оператором его отмены.

4.4.4 Заблокировать Ключ ЭП, уведомив Оператора по Системе ДО, по телефону, электронной почте или иным способом при условии возможности установления Оператором, что требование исходит от Клиента (путем Аутентификации Клиента).

5 СИСТЕМЫ И СЕРВИСЫ ДИСТАНЦИОННОГО ОБСЛУЖИВАНИЯ

5.1 Порядок обслуживания и использования ЭП в Системе ДО – Личный кабинет

5.1.1 Клиент для участия в ДО посредством системы Личный кабинет обязан обеспечить:

• Программное обеспечение: браузер, поддерживающий работу системы Личный кабинет:
- Edge 12 и выше;

- Firefox 52 и выше;

- Opera 44 и выше;

- Safari 10.1 и выше;

- Android Browser 67 и выше;

- Chrome 57 и выше.

• Персональный компьютер со следующими характеристиками:

- Процессор тактовой частотой не менее 2000Мгц, содержащий не менее 2 процессорных ядер;

- доступ к сети Интернет;

- оперативная память не менее 2048 Мб.

5.1.2 Клиент для доступа в Личный кабинет использует Логин и Пароль.

5.1.3 В случае если физическое лицо уже имеет Средства аутентификации, выданные Оператором или Банком-партнером ранее, то выдача новых не производится, и доступ к системе Личный кабинет осуществляется по уже имеющимся.

5.1.4 Клиент не должен сообщать Пароль и Одноразовые ключи третьим лицам, в т.ч. работникам Оператора, по телефону, электронной почте или иным способом. Использование Базовых аутентификационных данных и Одноразовых ключей допускается только при работе через сеть Интернет без участия работников Оператора.

5.1.5 Оператор направляет Одноразовые ключи Клиенту на Авторизованный номер, если Клиент не выбрал иной способ получения Одноразовых ключей.

Клиент вправе выбрать один из следующих способов получения Одноразовых ключей:

• Посредством СМС-сообщений на Авторизованный номер.

• Посредством Push-уведомлений на Авторизованный номер.

5.2 Восстановление доступа в Личный кабинет

5.2.1 В случае утраты/компрометации Базовых аутентификационных данных Клиента в Личный кабинет доступ может быть восстановлен путем предоставления Оператором Клиенту возможности самостоятельного дистанционного назначения нового Пароля.

5.2.2 В случае утраты /компрометации средств получения Одноразовых ключей (OTP-токена, мобильного телефона) восстановление доступа в систему происходит исключительно через сотрудника Оператора.

5.2.3 Восстановление доступа производится посредством Систем ДО на сайте в сети Интернет по адресу www.z.tochka.com путем совершения Клиентом юридически значимых действий для восстановления доступа в Систему ДО.

5.2.4 Восстановление Пароля в Личный кабинет осуществляется на сайте z.tochka.com при последовательном совершении Клиентом следующих действий:

Этап 1.

• вводит ФИО;

• вводит цифровое значение номера телефона, указанного в качестве Авторизованного номера;

При успешной проверке Оператором вышеперечисленных данных Клиент вводит Одноразовый ключ для подтверждения, отправленный Оператором в виде СМС-сообщения / Push-уведомления на Авторизованный номер или полученный Клиентом посредством OTP-токена.

Этап 2.

Вводит реквизиты Карты.

Этап 3.

Оператор отправляет уникальную одноразовую url-ссылку на адрес электронной почты, указанной Клиентом для восстановления доступа к Системе ДО. Ссылка действует ограниченное время.

Этап 4.

При переходе Клиента по ссылке, полученной на этапе 3 и срок действия которой не истек, Клиенту открывается окно сайта z.tochka.com и предлагается ввести новый пароль.

Этап 5.

После указания нового пароля, Клиент вводит Одноразовый ключ для подтверждения, отправленный Оператором в виде СМС-сообщения / Push-уведомления на Авторизованный номер или полученный Клиентом посредством OTP-токена.

При успешном прохождении всех этапов Клиенту в режиме реального времени назначается новый Пароль для доступа в Систему ДО.

Процедуру самостоятельного дистанционного восстановления Пароля могут пройти Клиенты, обладающие необходимыми данными. При отсутствии необходимых данных, Клиенты могут восстановить Пароль через сотрудника Оператора.

5.3 Обслуживание в Личном кабинете

5.3.1 Обслуживание в Системе ДО – Личный кабинет осуществляется на сайтах w w w . m y . t o c h k a . c o m и www.z.tochka.com. Требования, предъявляемые к защите информации на персональном компьютере (ином устройстве), приведены в Приложении к настоящим Правилам.

5.3.2 Все действия в Личном кабинете осуществляются только после формирования Клиентом ЭП с помощью Ключа ЭП и успешной проверки Оператором ЭП. Клиент, Оператор и Банк-партнер признают сформированную Клиентом и успешно проверенную Оператором в соответствии с настоящими Правилами ЭП равнозначной собственноручной подписи Клиента на документах, составленных на бумажном носителе.

5.3.3 Стороны признают, что используемые средства Личного кабинета исключают искажение ЭД при их обработке (передаче и хранении).

5.3.4 Для формирования ЭП Клиент должен обладать Ключом ЭП. Для проверки ЭП Оператору достаточно знать Сессионный ключ, Логин и Одноразовые ключи (при их наличии). ЭП формируется при совершении любой Операции и проставляется под каждым ЭД.

5.3.5 Формирование ЭП Клиентом осуществляется путем совершения последовательных действий в Личном кабинете, следуя инструкциям Оператора в экранных формах Личного кабинета при совершении Операции, при этом:

- Клиент производит Аутентификацию входа в Личный кабинет;

- Личный кабинет присваивает Клиенту Сессионный ключ, формируемый автоматически Личным кабинетом на основании введенных Клиентом Базовых аутентификационных данных или Дополнительных аутентификационных данных и Одноразового ключа;

- Клиент инициирует Операцию (вводит необходимые данные Операции) и передает Оператору электронное сообщение, содержащее информацию о Клиенте (Сессионный ключ) и Операции;

- Если операция предусматривает подтверждение Одноразовым ключом, Клиент, используя функциональные кнопки Личного кабинета, инициирует запрос получения Одноразового ключа посредством СМС-сообщения / Push-уведомления или генерирует самостоятельно, используя OTP-токен, в зависимости от выбранной клиентом Схемы Авторизации. Оператор имеет право определять необходимость использования Одноразовых ключей в зависимости от вида совершаемой операции или технических свойств Системы ДО.

- в случае использования Одноразового ключа посредством СМС-сообщения / Pushуведомления: Клиент обязан ознакомиться с поступившей в СМС-сообщении / Push-уведомлении с Одноразовым ключом информацией об Операции и, в случае согласия с описанием Операции, проводит Аутентификацию операции, вводя полученный Одноразовый ключ и подтверждая Операцию, используя функциональные кнопки Личного кабинета;

• в случае использования Одноразового ключа посредством OTP-токена: Клиент проводит Аутентификацию операции, вводя самостоятельно сгенерированный на OTP-токене Одноразовый ключ и подтверждая Операцию, используя функциональные кнопки в Личном кабинете;

• формируется ЭД и соответствующая ему ЭП.

5.3.6 Проверка ЭП производится Оператором в автоматическом режиме посредством Системы ДО в следующем порядке:

• Оператор проверяет в процессе Аутентификации входа представленные Базовые аутентификационные данные или Дополнительные аутентификационные данные;

• Оператор проверяет отсутствие факта отзыва со стороны Клиента Ключа ЭП до начала Сеанса связи с Оператором;

• Для проверки принадлежности Клиенту Сессионного ключа, Оператор, при необходимости, дополнительно запрашивает Одноразовый ключ;

• в случае использования Одноразового ключа, полученного Клиентом посредством СМС-сообщения / Push-уведомления, проверка Одноразового ключа осуществляется путем сравнения отправленного в СМС-сообщении / Push уведомлении Одноразового ключа, сгенерированного в Личном кабинете по запросу Клиента, с Одноразовым ключом, введенным Клиентом;

• в случае использования Одноразового ключа посредством OTP-токена проверка введенного Клиентом Одноразового ключа осуществляется в Личном кабинете по предоставленному производителем OTP-токенов закрытому алгоритму, с использованием серийного номера OTP-токена, значения кода, времени генерации кода;

• при отправке Клиентом в Личном кабинете ЭД, в автоматическом режиме отправляется также Сессионный ключ;

• при получении электронного сообщения по Операции Личный кабинет в автоматическом режиме проверяет соответствие полученного Сессионного ключа, имеющегося у Оператора. Для проверки принадлежности Клиенту Сессионного ключа, Оператор, при необходимости, дополнительно запрашивает Одноразовый ключ, который либо генерируется и направляется Клиенту в СМС-сообщении / Push-уведомлении с информацией об Операции, либо генерируется Клиентом самостоятельно посредством OTP-токена;

• в случае использования Одноразового ключа посредством СМС-сообщения / Push-уведомления: проверка Одноразового ключа осуществляется Личным кабинетом путем сравнения введенного Клиентом и отправленного Клиенту Одноразового ключа. Соответствие Одноразовых ключей на операцию (введенного Клиентов и отправленного Клиенту) подтверждает подлинность ЭП;

• в случае использования Одноразового ключа посредством OTP-токена: проверка сгенерированного Клиентом на OTP-токене и введенного Одноразового ключа осуществляется Личным кабинетом по предоставленному производителем OTP-токенов закрытому алгоритму, с использованием серийного номера OTP-токена, значения кода,

времени генерации кода. Успешная проверка Одноразового ключа подтверждает действительность ЭП.

5.3.7 Операция Банком-партнером осуществляется только после проверки Оператором корректности ЭП Клиента. Клиент признает, что технология работы с ОТР-токеном обеспечивает необходимый уровень безопасности работы с информацией, полученной посредством ОТР-токена, и исключает возможность несанкционированного Клиентом доступа третьих лиц к информации, полученной посредством ОТР-токена. Клиент признает, что номер ОТР-токена уникален, задан производителем, не может быть изменен и однозначно идентифицирует владельца ОТР-токена.

5.3.8 Клиент осознает, что, если по каким-либо причинам он не может воспользоваться ОТР-токеном, он вправе обратиться к Оператору, чтобы получить возможность использовать иной способ доступа к Счету Клиента.

5.3.9 Клиент обязуется хранить ОТР-токен в надежном месте, исключающем доступ к нему неуполномоченных лиц и повреждение материального носителя. В случае утери ОТР-токена Клиент обязан незамедлительно обратиться к Оператору лично либо по телефону с просьбой блокировать работу по всем своим Счетам и досрочно прекратить использование ОТР-токена.

5.3.10 ЭД, содержащий распоряжение Клиента о переводе денежных средств, исполняется Банком-партнером после проверки Оператором корректности ЭП Клиента.

5.4 Сервис Онлайн-консультант

5.4.1 Клиент, авторизованный для работы в Личном кабинете, имеет возможность вести электронную переписку с Оператором посредством услуги Онлайн-консультант. Стороны договорились, что любая переписка между Оператором и Клиентом в Личном кабинете посредством сервиса Онлайн-консультант считается обменом ЭД, подписанными ЭП Клиента. Такая переписка является юридически значимой, как если бы она осуществлялась на бумажных носителях с подписью Уполномоченных лиц.

5.4.2 Если из переписки в Онлайн-консультанте Личного кабинета Оператор установит волеизъявление Клиента, Оператор может сформировать, а Банк-партнер исполнить ЭД от имени Клиента в случае его подписания Клиентом посредством ЭП.

5.4.3 При получении электронного сообщения от Клиента в Онлайн-консультанте Оператор проверяет соответствие полученного Идентификатора Клиента имеющемуся у Оператора Идентификатору Клиента в Личном кабинете. Соответствие полученного и имеющегося Идентификатора Клиента расценивается Личным кабинетом как подтверждение подлинности ЭП.

5.4.4 Клиент обязан вести переписку посредством сервиса Онлайн-консультант в корректной форме, без использования оскорбительных и нецензурных выражений, непристойных фраз и бранных слов, а также соблюдать общепринятые морально-этические нормы общения.

5.4.5 В случае неисполнения Клиентом обязанности, предусмотренной п. 5.4.4. Оператор вправе уведомить Клиента о недопустимости ведения дальнейшей переписки в некорректной форме.

5.4.6 В случае повторного, либо неоднократного нарушения Клиентом условий ведения переписки Оператор вправе на неопределенный срок по своему усмотрению ограничить доступ Клиента к услуге Онлайн-консультант, предварительно уведомив об этом Клиента.

5.4.7 Ограничение доступа к услуге Онлайн-консультант не влечет за собой наложения каких-либо иных ограничений на использование Клиентом любых других функций, сервисов и услуг, доступных в Системе ДО, кроме возможности ведения переписки с Оператором посредством услуги Онлайн-Консультант. При этом Стороны признают, что в любой момент, вне зависимости от наличия ограничения на пользование данной услугой, либо его отсутствия, Клиент вправе обратиться к Оператору, воспользовавшись сервисом Колл-центр.

5.4.8 Оператор оставляет за собой право в любой момент по собственному усмотрению восстановить Клиенту возможность использования услуги Онлайн-консультант без предварительного уведомления Клиента.

5.5 Сервис Facebook_bot

5.5.1 Для использования Facebook_bot Клиенту необходимо:

- быть пользователем Системы ДО: Личный кабинет и/или Система «Точка»,
- самостоятельно установить соответствующее приложение Facebook, которое доступно в официальном репозитории мобильных приложений или воспользоваться веб-версией Facebook;
- зарегистрироваться в Facebook;
- в Facebook найти пользователя в поисковой строке с именем @bankTochka в случае использования мобильного приложения Facebook или найти в поисковой строке найти страницу пользователя с именем Точка, расположенной по адресу в сети Интернет www.facebook.com/bankTochka/ в случае использования веб-версии Facebook.

5.5.2 Для отправки запросов Оператору посредством Facebook_bot необходимо пройти процедуру Авторизации, для чего необходимо совершить следующие действия:

- Зайти на страницу пользователя с именем Точка
- Выбрать функцию меню «Отправить сообщение»
- Следуя экранным формам использовать функционал бота, не требующий авторизации либо выбрать пункт «Авторизоваться» или «Log In»
- Бот переадресует на страницу https://bot.tochka.com/auth и предложит ввести Базовые аутентификационные данные
- В случае успешной проверки введенных данных Клиенту станет доступен функционал авторизованного пользователя.

5.5.3 После прохождения процедуры Авторизации устанавливается Сеанс связи Клиента с Оператором посредством интерфейса Facebook и становится доступным следующий функционал:

- Реквизиты Счетов

• Запрос баланса по Счетам

• Последние операции по Счетам

• Повтор платежей с возможностью изменения суммы и назначения платежа

• Онлайн-консультант

5.5.4 Все сообщения, отправляемые Клиентом после прохождения процедуры Авторизации, считаются подписанными ЭП Клиента.

5.5.5 Формирование ЭП Клиентом осуществляется после успешной Аутентификации входа путем совершения Клиентом последовательных действий:

• Клиенту присваивается Сессионный ключ, формируемый автоматически Системой ДО на основании правильно введенных Клиентом Базовых аутентификационных данных;

• Сессионный ключ содержится в каждом запросе Клиента, направляемом в Facebook_bot.

5.5.6 Проверка принадлежности Клиенту ЭД, полученного Оператором посредством Facebook_bot, производится Оператором после получения ЭД и проверки корректности Сессионного ключа Клиента.

5.5.7 Проверка ЭП производится Оператором в порядке, определенном для Систем ДО Личного кабинета и Система «Точка».

5.6 Сервис Мессенджер

5.6.1 Для использования Мессенджера Клиенту необходимо:

• быть пользователем Системы ДО Личного кабинета и/или Система «Точка»;

• самостоятельно установить соответствующее приложение для Портативного устройства, которое доступно в официальном репозитории мобильных приложений или воспользоваться его веб-интерфейсом (при наличии);

• быть зарегистрированным пользователем в соответствующем Мессенджере;

• в Мессенджере Telegram необходимо открыть ссылку https://t.me/Bank_TochkaBot, либо найти пользователя в поисковой строке с именем «Банк Точка»;

• в Мессенджере Viber необходимо открыть ссылку viber://pa?chatURI=bank_tochka (пользователь «Банк Точка»). В поисковой строке пользователь с таким именем не отражается в связи политикой компании-правообладателя.

5.6.2 Для отправки запросов Оператору посредством Мессенджера, Клиенту необходимо пройти процедуру Авторизации, для чего необходимо совершить следующие действия:

• В Мессенджере открыть чат с пользователем «Банк Точка»;

• В строке для сообщений набрать и отправить команду /connect;

• Перейти по ссылке, направленной пользователем «Банк Точка» в ответ на команду /connect;

• Пройти процедуру Авторизации в соответствии с указаниями интерфейса.

5.6.3 В случае успешного прохождения Клиентом процедуры Авторизации, устанавливается соответствие Базовых аутентификационных данных Клиента у Оператора идентификатору Клиента в соответствующем Мессенджере.

5.6.4 При выполнении Клиентом всех условий, указанных в п 6.6.1 – 6.6.3 настоящего раздела Правил, устанавливается Сеанс связи Клиента с Оператором посредством интерфейса Мессенджера, и становится доступным функционал услуги Онлайн-консультант, в соответствии с п 6.4. настоящего раздела Правил.

5.6.5 Все сообщения, отправляемые Клиентом после прохождения процедуры Авторизации, считаются подписанными ЭП Клиента.

5.6.6 Проверка принадлежности Клиенту ЭД, полученного Оператором посредством Мессенджера, производится оператором после получения ЭД и идентификатора Клиента в соответствующем Мессенджере.

5.6.7 Все сообщения, направляемые Клиентом посредством соответствующего Мессенджера и ответы Оператора на них, становятся доступными для просмотра в интерфейсе Системы ДО: Личный кабинет и/или Система «Точка».

5.6.8 В случае, если после прохождения процедуры Авторизации, Клиент не направляет посредством соответствующего Мессенджера сообщения/команды Оператору в течение 30 календарных дней, то Сеанс связи считается прерванным, а Авторизация прекращенной.

5.6.9 Клиент вправе в любой момент времени в одностороннем порядке прервать Сеанс связи и прекратить Авторизацию в соответствующем Мессенджере, набрав и отправив в строке для сообщений команду /disconnect/.

5.7 Сервис «Персональная страница вашей компании»

5.7.1 Оператор предоставляет Клиенту возможность посредством системы Личный кабинет, воспользоваться услугой «Персональная страница вашей компании». В процессе оказания услуги, Клиент - юридическое лицо или индивидуальный предприниматель, используя интерфейс системы Личный кабинет, получает возможность создания и последующего размещения по уникальной ссылке на сайте Оператора в сети «Интернет» по адресу: http://tochka.com, web-страницы, которая содержит следующую информацию и функционал:

• Раздел «Реквизиты компании» - содержит в себе юридические и платежные реквизиты Клиента;

• Вкладка «Заплатить» - предоставляет два способа осуществления платежей в пользу Клиента:

(i) по правилам услуги c2c;

(ii) путем создания файла с платежным документом и его загрузки на компьютер отправителя;

• Вкладка «Выставить счет» - позволяет создать платежный документ, посредством заполнения необходимых реквизитов, который впоследствии будет доступен для оплаты в Системе ДО Клиента.

5.7.2 Клиент осуществляет активацию услуги во вкладке «Профиль» в Личном кабинете. Активировав услугу Клиент может осуществлять следующие действия:

5.7.2.1 Изменять ссылку на web-страницу услуги;

5.7.2.2 Отправлять и опубликовывать ссылку по своему усмотрению через социальные сети, либо электронным письмом, либо копировать ссылку.

5.7.2.3 Активировать вкладку «Выставить счет». Активируя данную вкладку Клиент понимает и принимает риск получения на подпись в Системе ДО платежных документов извне от третьих лиц, и обязуется проверять перед подписанием ЭП обоснованность и достоверность данных платежных документов.

5.7.2.4 Опубликовывать на web-странице Услуги дополнительную информацию о Клиенте по собственному усмотрению.

5.7.3 Осуществив активацию услуги Клиент осознает и принимает риск получения третьими лицами информации о персональных данных Клиента, реквизитах его банковского счета и иной конфиденциальной информации, указанной на web-странице Услуги.

5.8 Порядок обслуживания и использования ЭП в Системе «Точка»

5.8.1 Система «Точка» - Система ДО.

5.8.2 Клиент может воспользоваться Системой «Точка» с помощью устройства, работающего под управлением операционной системы iOS или Android, подключенного к сети Интернет, самостоятельно установив Мобильное приложение «Точка». Мобильное приложение Клиент должен найти в официальном онлайн-магазине мобильных приложений и установить на Портативное устройство.

5.8.3 Активация доступа в Мобильном приложении:

• После запуска Мобильного приложения, на экране устройства отобразится страница входа.

• Клиент вводит с использованием цифровой клавиатуры Базовые аутентификационные данные. Ввод корректных Базовых аутентификационных данных является основанием для начала обслуживания в Системе ДО.

• На основании введенных Базовых аутентификационных данных, Оператор присваивает Клиенту Идентификатор Клиента.

• После Активации Клиент самостоятельно задает Цифровой код, который, по сути, является Ключом простой ЭП, и который Клиент обязан держать в секрете от третьих лиц, соблюдать его конфиденциальность.

• После создания Цифрового кода, Система «Точка» предложит Клиенту установить альтернативный способ Аутентификации входа – по Touch ID коду (если Портативное устройство поддерживает данную технологию).

• Все последующие входы в Систему «Точка» осуществляются посредством Аутентификации входа по Цифровому коду либо Аутентификации входа по Touch ID коду.

5.8.4 В случае последовательного трехкратного ввода неверного Цифрового кода или Touch ID кода, Активация аннулируется. Клиент обязан заново пройти процедуру Активации.

5.8.5 В случае утраты Цифрового кода, доступ в Систему «Точка» осуществляется путем сброса текущей Активации в Мобильном приложении. Для этого на экране входа в Мобильном приложении Клиент должен нажать на функциональную кнопку «Забыли код?», подтвердить сброс Цифрового кода и повторно пройти процедуру Активации.

5.8.6 Оператор имеет право определять необходимость использования Одноразовых ключей в зависимости от различных критериев, устанавливаемых Оператором.

5.8.7 В Системе «Точка» существует возможность просмотра информации без ввода Цифрового кода. Такая опция позволяет Клиенту осуществлять просмотр информации, доступной в приложении. Для совершения иных действий Клиенту необходимо ввести Цифровой код. Клиент может самостоятельно менять настройки, по отключению/включению использования Цифрового кода на просмотр информации в приложении, следуя экранным формам приложения. Данный функционал доступен при условии наличия на Портативном устройстве Клиента соответствующей версии Мобильного приложения.

5.8.8 Клиент осознает и принимает риски, связанные с отменой Цифрового кода. В случае утери/кражи или выбытия Портативного устройства по иному основанию помимо воли Клиента, третьи лица могут получить доступ к следующей информации: о номере счета/счетов Клиента, об остатках и движении денежных средств по счету/счетам, наличии выпущенных Банковских карт, их количестве, номерах, сроке действия, действующим по Банковской карте лимитам, фамилии, имени, отчества владельца счета и держателя карты, наименование организации, которой принадлежит счет.

5.8.9 Оператор не несет ответственность в случае наступления негативных последствий, связанных отменой клиентом Цифрового кода для просмотра информации в Системе «Точка».

5.8.10 В целях обеспечения безопасности исполнение ЭД Клиента осуществляется только после формирования Клиентом ЭП с помощью Ключа ЭП и успешной проверки ЭП Оператором.

5.8.11 Формирование ЭП Клиентом осуществляется после успешной Аутентификации входа путем совершения Клиентом последовательных действий:

• Клиент открывает Систему «Точка»;

• Осуществляется Аутентификация входа;

• Система «Точка» присваивает Клиенту Сессионный ключ, формируемый автоматически Системой «Точка» на основании введенного Клиентом Цифрового кода/Touch ID кода;

• Клиент инициирует Операцию (вводит необходимые данные Операции) и передает Оператору электронное сообщение, содержащее информацию о Клиенте (Сессионный ключ) и Операции;

• В случае использования Одноразовых ключей, Клиент инициирует запрос получения Одноразового ключа посредством СМС-сообщения / Push-уведомления, вводит в форму Приложения полученный Одноразовый ключ, тем самым подтверждая Операцию;

• В случае использования Цифрового кода/ Touch ID, инициирует проверку Цифрового кода/ Touch ID кода, используя функциональные кнопки Системы «Точка»;

• В случае использования Одноразового ключа посредством СМС-сообщения / Push-уведомления: Клиент обязан ознакомиться с поступившей в СМС-сообщении / Push-уведомлении с Одноразовым ключом информацией об Операции и, в случае согласия с описанием Операции, проводит Аутентификацию операции, вводя полученный Одноразовый ключ и подтверждая Операцию, используя функциональные кнопки Системы «Точка»;

• Система «Точка» передает электронное сообщение по Операции вместе с Сессионным ключом Оператору;

• Проверка принадлежности Клиенту ЭД, полученного Оператором посредством Системы «Точка», производится Оператором после получения ЭД, проверка корректности Сессионного ключа Клиента и Одноразового ключа/Цифрового кода/Touch ID;

5.8.12 Проверка ЭП производится Оператором следующим образом:

• Оператор проверяет в процессе Аутентификации входа в Систему «Точка» введенный Клиентом Цифровой код/Touch ID код;

• при отправке Клиентом ЭД в Системе «Точка», вместе с ЭД в автоматическом режиме отправляется также Сессионный ключ;

• при получении ЭД от Клиента Система «Точка» в автоматическом режиме проверяет соответствие полученного Сессионного ключа, имеющегося у Оператора. Для проверки принадлежности Клиенту Сессионного ключа, Оператор дополнительно запрашивает либо Одноразовый ключ, который либо генерируется и направляется Клиенту в СМС-сообщении / Push-уведомлении с информацией об Операции, либо Цифровой код/Touch ID код, который Клиент вводит на экранных формах Мобильного приложения;

• в случае использования Одноразового ключа посредством СМС-сообщения/ Push-уведомления проверка Одноразового ключа осуществляется Системой «Точка» путем сравнения введенного Клиентом и отправленного Клиенту Одноразового ключа. Соответствие Одноразовых ключей на операцию (введенного Клиентов и отправленного Клиенту) подтверждает подлинность ЭП;

• в случае использования Цифрового кода/Touch ID кода осуществляется проверка корректности введенного Цифрового кода/Touch ID кода.

5.8.13 В Системе «Точка» Оператором предусмотрена опция для Клиентов «Защищенный сеанс связи с Оператором путем совершения телефонного звонка». Для совершения звонка совершаются следующие действия:

• Производится Аутентификация входа в Системе «Точка»;

• Клиент инициирует телефонный звонок Оператору, следуя инструкциям экранных форм Системы «Точка»;

• Система «Точка», запросив подтверждение Клиента, инициирует звонок на номер телефона Оператора с последующим автоматическим набором полученного от Оператора Одноразового ключа в тональном режиме;

• Оператор проверяет корректность полученного в телефонном сеансе Одноразового ключа. В случае совпадения значений Одноразового ключа, переданного Оператором в Систему «Точка» и полученного Оператором в телефонном сеансе, звонок признается

инициированным Клиентом, а Клиент считается Авторизованным, с присвоенным Сессионным ключом, полученным при Аутентификации сессии в Систему «Точка».

• В результате успешного совершения описанных действий Клиент вправе вести с Оператором переговоры, давать обязательные для выполнения указания, в том числе на совершение операций.

• Клиент, авторизованный на работу в Системе «Точка», имеет возможность вести электронную переписку с Оператором посредством сервиса Онлайн-консультант. Для использования Клиентом сервиса совершаются следующие действия:

- Производится Аутентификация входа в Системе «Точка».

- Клиент инициирует начало электронной переписки, следуя инструкциям экранных форм Системы «Точка».

- Клиент создает сообщение, которое Система «Точка» отправляет Оператору вместе с Сессионным ключом.

- При получении электронного сообщения от Клиента посредством сервиса Онлайн-консультант в Системе «Точка» Оператор проверяет корректность Сессионного ключа Клиента.

5.8.14 Стороны договорились, что любая переписка в Системе «Точка» посредством сервиса Онлайн-консультант между Оператором и Клиентом считается обменом ЭД, подписанными ЭП Клиента. Соответствие полученного и имеющегося Сессионного ключа Клиента расценивается Системой «Точка» как проверка действительности ЭП. Клиент не может передавать, а Оператор принимать поручения на перевод денежных средств посредством Онлайн-консультанта в Системе «Точка».

5.8.15 Оператор может формировать ЭД от имени Клиента или исполнять заявления Клиента в Системе «Точка», если из переписки в Онлайн-Консультанте в Системе «Точка» Оператор установит волеизъявление Клиента. При этом Клиент несет ответственность за правильность, достаточность сообщенных Оператору реквизитов для совершения Банком-партнером перевода.

5.8.16 Стороны признают переписку в Онлайн-Консультанте в Системе «Точка» юридически значимой, как если бы переписка осуществлялась на бумажных носителях с подписью Уполномоченных лиц.

5.9 Сервис «Робопин»

5.9.1 Пользование Сервисом «Робопин» позволяет Клиенту посредством телефонной связи:

• установить ПИН-код к Банковской карте;

• изменить ПИН-код к Банковской карте.

5.9.2 Для получения услуги в Сервисе «Робопин» Клиенту необходимо последовательно выполнить следующие действия:

• посредством телефонной связи позвонить по номеру +7-800-2000-024, опубликованному на сайте www.tochka.com, с Авторизованного номера Клиента;

• сообщить оператору в устной форме о намерении установить или изменить ПИН-код к Банковской карте;

• пройти процедуру идентификации, которая производится Оператором в соответствии с внутренними регламентными документами Оператора.

5.9.3 При успешной идентификации оператор переключает Клиента на Сервис «Робопин» в рамках текущего телефонного Сеанса связи. После переключения Клиент:

• после запроса Сервиса «Робопин» вводит с Авторизованного номера телефона в тональном режиме значение ПИН-кода;

• если значение ПИН-кода соответствует требованиям безопасности, установленным Оператором, Клиент повторно вводит значение ПИН-кода;

• если значение ПИН-кода не соответствует требованиям безопасности, установленным Оператором, Клиент должен ввести другое значение ПИН-кода.

• При успешном выполнении вышеперечисленных действий в режиме реального времени меняется значение ПИН-кода к Банковской карте Клиента.

6 ПРИОСТАНОВЛЕНИЕ, ВОЗОБНОВЛЕНИЕ И ПРЕКРАЩЕНИЕ ОБСЛУЖИВАНИЯ В СИСТЕМЕ ДО

6.1 Приостановление обслуживания Клиента в Системе ДО

6.1.1 Приостановление обслуживания Клиента в Системе ДО подразумевает прекращение приема ЭД Клиента к рассмотрению (исполнению) во всех составляющих (видах) Системы ДО, за исключением возможности вести переписку посредством систем ДО с Оператором, кроме случаев, установленных настоящим разделом.

6.1.2 Приостановление обслуживания Клиента в Системе ДО может происходить:

• по инициативе Оператора;

• по инициативе Клиента;

• независимо от воли Сторон, если приостановление вызвано факторами непреодолимой силы и/или чрезвычайными обстоятельствами (в т.ч. стихийными явлениями, военными действиями, актами органов власти).

6.1.3 Убытки Клиента, возникшие в связи с приостановлением доступа Клиента к Системам ДО, как по инициативе Клиента, так и по инициативе Оператора и/или Банка-партнера, возмещению не подлежат.

6.2 Основаниями для приостановления обслуживания Клиента в Системе ДО по инициативе Оператора являются:

6.2.1 Несоблюдение Клиентом требований к обмену ЭД предусмотренных действующим законодательством РФ и условиями настоящих Правил.

6.2.2 Непроведение Сеансов связи с Оператором в течение более 3 (трех) месяцев подряд, а именно: Клиент не совершает Аутентификацию входа с целью получения информации об остатках денежных средств на Счетах, регистрации и исполнения ЭД, не совершает иных действий по использованию Систем ДО.

6.2.3 Образование задолженности по оплате услуг Клиента перед Оператором в соответствии с Тарифами Оператора.

6.2.4 В случае возникновения у Оператора технических неисправностей или других обстоятельств, препятствующих использованию Систем ДО до устранения возникших обстоятельств. О возникшем сбое (неисправности) и предполагаемых сроках его устранения Оператор оповещает Клиента через Системы ДО или путем публикации информации на Сайте.
6.2.5 Оператору стало известно о следующих признаках, указывающих на изменение:

6.2.5.1 получателя информации, направленной Оператором и используемой при Аутентификации входа в Системы ДО;

6.2.5.2 владельца SIM-карты Клиента, прекращении обслуживания или смене Авторизованного номера телефона.

6.2.6 Компрометация ЭП в случае уведомления Оператора Клиентом в порядке, предусмотренном настоящими Правилами.

6.2.7 Наличие у Оператора оснований считать, что возможно несанкционированное использование Систем ДО от имени Клиента.

6.2.8 Возникновение конфликта, который не позволяет достоверно определить полномочия лиц, ответственных за обмен ЭД от имени Клиента.

6.2.9 Получение Оператором информации о смерти Владельца ЭП.

6.2.10 Проведение Оператором замены программного обеспечения или аппаратных средств, или проведение регламентных работ.

6.2.11 Получение информации от Банка-партнера о необходимости приостановления обслуживания по основаниям, предусмотренным Правилами банковского обслуживания.

6.2.12 Иные основания, предусмотренные настоящими Правилами и действующим законодательством РФ.

6.2.13 Опеатор уведомляет Клиента о приостановлении обслуживания в системе ДО по любому, согласованному с Клиентом, каналу связи или путем направления ЭД с указанием причин, даты начала и срока приостановления участия в обмене ЭД.

6.2.14 В случае проведения Оператором замены программного обеспечения или аппаратных средств или проведения регламентных работ Оператор предварительно, не менее чем за 2 (Два) часа, уведомляет Клиентов путем размещения соответствующей информации на web-сайте www.tochka.com или путем направления соответствующего электронного сообщения по системе ДБО.

6.3 Основаниями для приостановления обслуживания в Системе ДО по инициативе Клиента являются:

6.3.1 Заявление Клиента о приостановлении обслуживания в Системе ДО. Заявление может быть передано по телефону, электронной почте или иным способом при условии, что на основании представленной Клиентом Оператору информации у Оператора не возникает сомнений, что заявление исходит от Клиента.

6.3.2. Заявление Клиента о возможности Компрометации Ключей ЭП. Заявление может быть передано по телефону, электронной почте или иным способом при условии, что на основании представленной Клиентом Оператору информации у Оператора не возникает сомнений, что заявление исходит от Клиента.

6.4 Основаниями прекращения обслуживания Клиентов в Системе ДО являются:

6.4.1 Расторжение Договора по инициативе любой из Сторон.

6.4.2. В иных случаях, предусмотренных действующим законодательством и настоящими Правилами.

6.5 Возобновление обслуживания в Системе ДО

6.5.1 Оператор вправе в любой момент возобновить ДО по собственной инициативе, если причина, по которой оно было приостановлено или ограничено, перестала существовать.

6.5.2 В остальных случаях - для возобновления доступа к Системе ДО Клиент должен предоставить Оператору заявление в свободной форме с просьбой возобновить работу по Системе ДО, если у Клиента существует возможность переписки с Оператором. В случае, если возможность переписки с Оператором по системе ДО у Клиента отсутствует, то Оператор для принятия Заявления производит выезд к Клиенту. При этом Оператор принимает решение о восстановлении/не восстановлении предоставления услуг в течение 5 (Пяти) рабочих дней с даты предоставления Клиентом заявления.

6.5.3 Оператор вправе отказать в возобновлении обслуживания в случае нарушения Клиентом обязательств, предусмотренных настоящими Правилами до устранения Клиентом таких обстоятельств.

7 ОТВЕТСТВЕННОСТЬ СТОРОН ПРИ ИСПОЛЬЗОВАНИИ СИСТЕМ ДО. ОСНОВАНИЯ ОСВОБОЖДЕНИЯ ОТ ОТВЕТСТВЕННОСТИ

7.1 Клиент несет ответственность за содержание любого ЭД, подписанного ЭП лиц, ответственных за обмен ЭД от имени Клиента.

7.2 Сторона, несвоевременно сообщившая о случаях компрометации средства ЭП или ЭП, несет связанные с этим риски возникновения убытков.

7.3 Стороны не несут ответственность за убытки, понесенные одной Стороной не по вине другой Стороны в результате использования Систем ДО, в том числе при исполнении ошибочных ЭД, если переданные ЭД были оформлены надлежащем образом, подписаны ЭП, а Оператором получены, проверены и признаны верными.

7.4 Оператор не несет ответственность за ущерб, возникший:

7.4.1 вследствие компрометации по вине Клиента Аутентификационных данных и (или) Одноразовых паролей (при их использовании), их утраты или несанкционированного доступа к ним и их использования третьими лицами;

7.4.2 в случае нарушения Клиентом Договора;

7.4.3 вследствие принятия высшими органами законодательной и исполнительной власти Российской Федерации решений, которые делают невозможным для Оператора выполнение своих обязательств по Договору;

7.4.4 вследствие сбоев в работе линий связи, обрыва линий связи, выхода из строя оборудования у телефонного оператора и/или оператора доступа к сети Интернет;

7.4.5 в случае несанкционированного подключения к Системам ДО и получения доступа к Счету третьих лиц, с использованием Авторизованного номера телефона Клиента, если такой доступ имел место не по вине Оператора.

7.5 Оператор не несет ответственность за качество линий связи.

7.6 Оператор не несет ответственность за невозможность направления Клиенту СМС-сообщений/Push-уведомлений в случае, если такая невозможность вызвана сменой Авторизованного номера Клиентом и неуведомлением Оператора о данном обстоятельстве, действиями либо бездействием Клиента и (или) оператора сотовой связи в рамках имеющихся между Клиентом и оператором сотовой связи правоотношений, а также связана с иными действиями Клиента, оператора сотовой связи и иного третьего лица или иными причинами, находящимися вне сферы контроля Оператора. Оператор не несет ответственности за любые убытки, понесенные Клиентом в результате действия или бездействия оператора сотовой связи либо иного третьего лица. Иск может быть предъявлен фактическому виновнику убытков, исключая Оператора.

7.7 Клиент уведомлен и согласен с тем, что невозможность представить ЭП, осуществить иное действие посредством систем ДО, не может служить основанием для освобождения Клиента от ответственности за неисполнение или ненадлежащее исполнение обязательств перед Оператором по Договору или иным договорам, заключенным между Оператором и Клиентом.

7.8 Оператор не несет ответственности за повторную ошибочную передачу ЭД Клиентом.

7.9 Оператор не несет ответственности за невыполнение, несвоевременное или неправильное выполнение ЭД Клиента, если это было вызвано предоставлением Клиентом недостоверной информации, вводом неверных данных и/или несвоевременным информированием Оператора об изменениях в данных, сообщенных Оператору ранее.

7.10 Клиент осознает и принимает все возможные риски, связанные с размещением шаблона расчетного документа в Системе ДО, в том числе риск использования и размещения персональных данных Клиента. Также Клиент осознает, что Оператор не несет ответственности за правильность указанных в шаблоне реквизитов расчетного документа в том случае, если шаблон расчетного документа размещен в Системе ДО другим Клиентом Оператора, равно как Оператор не несет ответственности за осуществление Клиентом платежа с использованием шаблона расчетного документа, размещенного другим Клиентом Оператора.

7.12 В случае если Клиент пользуется сервисами третьих лиц, которые интегрированы с Системой ДО, Клиент дает свое согласие на передачу соответствующему сервису всей информации о Клиенте, связанной с использованием соответствующего сервиса. При этом Клиент осознает, что Оператор не несет ответственности за доступ третьих лиц к любой информации, передаваемой в рамках использования Клиентом сервисов, интегрированных с Системой ДО Клиента.

8 ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ С ИСПОЛЬЗОВАНИЕМ СИСТЕМ ДО

8.1 Возникновение спорных ситуаций при использовании Систем ДБО

8.1.1 Для целей настоящего раздела под спорной ситуацией понимается существование у Сторон претензий по действиям и операциям, проводимым с использованием Систем ДО.

8.1.2 Действие настоящего раздела Правил не распространяется на физических лиц, не обладающих статусом индивидуального предпринимателя или лиц, занимающихся в установленном законодательством порядке РФ частной практикой.

8.2 Уведомление о спорной ситуации

8.2.1 В случае несогласия Клиента с действиями Банка-партнера, Клиент не позднее дня, следующего за днем получения информации о совершенной операции по Счету, направляет посредством Систем ДО письменное уведомление о своем несогласии с проведенной операцией (далее - Претензия). Претензия, направленная за пределами, установленного в настоящем пункте срока, рассмотрению не подлежит, а совершенные операции и остаток средств на счете считаются подтвержденными (одобренными) Клиентом. В Претензии должно быть изложено существо возражений с указанием на ЭД с ЭП, на основании которого возникла спорная ситуация или с исполнением которого Клиент не согласен, и обстоятельствах, которые, по мнению составителя, свидетельствуют о наличии спорной ситуации. Претензия должна содержать все реквизиты ЭД, предусмотренные ПБО.

8.2.2 После получения Претензии Оператор вправе запросить у Клиента подтверждение факта владения ОТП-Токеном, Авторизованным номером для установления факта соблюдения порядка и мер безопасности по их использованию в соответствии с настоящими Правилами.

8.2.3 Клиент обязан не позднее 3 (Трех) рабочих дней с момента направления требования представить в Оператору используемые им электронные средства платежа.
8.2.4 Оператор, как организатор ИС, в течение 30 (Тридцати) календарных дней проверяет наличие обстоятельств, свидетельствующих о возникновении спорной ситуации, и направляет Клиенту Заключение о результатах проведенной проверки (Заключение Оператора).
8.2.5 В случае если Клиент не согласен с выводами, изложенными в Заключении Оператора, для рассмотрения спорной ситуации может быть сформирована Разрешительная комиссия.

8.2.6 Для формирования Разрешительной комиссии Клиент не позднее дня, следующего за днем получения от Оператора Заключения, направляет Оператору требование о формировании Разрешительной комиссии (далее – Требования Клиента о формировании Разрешительной комиссии).

8.3 Формирование Разрешительной комиссии, ее состав и сроки рассмотрения споров

8.3.1 Не позднее 3 (Трех) рабочих дней с момента получения Требования Клиента о формировании Разрешительной комиссии формируется Разрешительная комиссия.

8.3.2 Разрешительная комиссия формируется с участием уполномоченных представителей от каждой Стороны. В состав Разрешительной комиссии входит по одному уполномоченному представителю от Клиента, Оператора и Банка-партнера.

8.3.3 Назначаются время, место, дата и участники (уполномоченные представители) проведения процедуры разрешения спора.

8.3.4 Неявка Клиента или его представителя для участия в процедуре разрешения спора на Разрешительную комиссию не является препятствием для ее проведения.

8.3.5 Разрешительная комиссия в составе уполномоченных представителей Сторон должна состояться не позднее 45 (Сорока пяти) календарных дней с момента получения Оператором Требования о ее формировании.

8.4. Компетенция и полномочия Разрешительной комиссии

8.4.1 Участники Разрешительной комиссии проводят процедуру разрешения спора с изучением представленных Сторонами спора доказательств, рассматривают

представленное Оператором Заключение. Разрешительная комиссия устанавливает наличие или отсутствие фактических обстоятельств, свидетельствующих о факте и времени составления и/или отправки ЭД, его подлинности, а также о подписании ЭД конкретной ЭП, аутентичности отправленного Клиентом ЭД полученному Банком-партнером.

8.4.2 Разрешительная комиссия вправе рассматривать любые иные технические вопросы, необходимые, по мнению Разрешительной комиссии, для выяснения причин и последствий возникновения спорной ситуации.

8.4.3 Все члены Разрешительной комиссии имеют по одному голосу. Решение Разрешительной комиссии принимаются большинством голосов.

8.4.4 Результатом рассмотрения спорной ситуации Разрешительной комиссией является определение авторства ЭД и действительности ЭП Клиента.
8.4.5 По итогам работы Разрешительной комиссии составляется Акт, в котором содержится изложение выводов Разрешительной комиссии.

8.5 Передача спора на рассмотрение в суд

8.5.1 В случае несогласия с решением Разрешительной комиссии спор передается заинтересованной Стороной на рассмотрение в суд.

8.5.2 Стороны договорились, что при рассмотрении спора в суде обязательным доказательством по делу является Заключение Оператора.

8.5.3 В случае, если стороной в споре является Клиент – физическое лицо, не обладающее статусом индивидуального предпринимателя или лица, занимающегося в установленном законодательством порядке РФ частной практикой, соблюдение установленного настоящим разделом порядка разрешения споров не является обязательным. Такой Клиент вправе для разрешения спора обратиться непосредственно в суд.

9 АНТИКОРРУПЦИОННАЯ ОГОВОРКА

9.1 При исполнении своих обязательств по Договору, Стороны, их аффилированные лица, работники или посредники не выплачивают, не предлагают выплатить и не разрешают выплату каких-либо денежных средств или ценностей, прямо или косвенно, любым лицам, для оказания влияния на действия или решения этих лиц с целью получить какие-либо неправомерные преимущества или иные неправомерные цели.

9.2 При исполнении своих обязательств по Договору, Стороны, их аффилированные лица, работники или посредники не осуществляют действия, квалифицируемые применимым для целей Договора законодательством, как дача/получение взятки, коммерческий подкуп, а также действия, нарушающие требования применимого законодательства и международных актов о противодействии легализации (отмыванию) доходов, полученных преступным путем.

9.3 В случае возникновения у Стороны подозрений, что произошло или может произойти нарушение каких-либо положений предыдущего пункта, соответствующая Сторона обязуется уведомить другую Сторону в письменной форме.

9.4 В письменном уведомлении Сторона обязана сослаться на факты или предоставить материалы, достоверно подтверждающие или дающие основание предполагать, что произошло или может произойти нарушение каких-либо положений настоящего раздела контрагентом, его аффилированными лицами, работниками или посредниками

выражающееся в действиях, квалифицируемых применимым законодательством, как дача или получение взятки, коммерческий подкуп, а также действиях, нарушающих требования применимого законодательства и международных актов о противодействии легализации доходов, полученных преступным путем.

9.5 После письменного уведомления, соответствующая Сторона имеет право приостановить исполнение обязательств по Договору до получения подтверждения, что нарушения не произошло или не произойдет. Это подтверждение должно быть направлено в течение десяти рабочих дней с момента направления письменного уведомления.

10 ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

1 Стороны обязуются уведомлять друг друга об изменении своего места нахождения, а также об изменении иных реквизитов, имеющих существенное значение для определения юридического статуса Сторон.

2 Перечень третьих лиц, в отношении которых Клиент дает согласие на обработку его персональных данных в целях продвижения услуг Оператора, Банков-партнеров, совместных услуг Оператора и третьих лиц, продуктов (товаров, работ, услуг) третьих лиц, осуществления почтовых рассылок:

- Акционерное общество «Открытие Брокер», местонахождение: 115114, г. Москва, ул. Летниковская, д. 2, стр. 4;
- Общество с ограниченной ответственностью «Управляющая компания «ОТКРЫТИЕ», местонахождение: 115114, г. Москва, пер. Дербеневский 1-й, д. 5, стр. 2;
- Акционерное общество «Открытие Холдинг», местонахождение: 115114, г. Москва, ул. Летниковская, д. 2, стр. 4;
- Общество с ограниченной ответственностью «Платформа Финанс», местонахождение: 123100, г. Москва, набережная Краснопресненская, д. 6;
- Закрытое акционерное общество "АККОРД ПОСТ", местонахождение: 113452, г. Москва, ул. Азовская, д. 31;
- ФГУП «Почта России», местонахождение: 131000, г. Москва, Варшавское шоссе, д. 37;
- Открытие акционерное общество «Мегафон», местонахождение: 115035, г. Москва, Кадашевская набережная, д.30;
- Общество с ограниченной ответственностью Небанковская кредитная организация «Рапида», местонахождение: 125315, г. Москва, ул. Усиевича, д.20, корп.2;
- Общество с ограниченной ответственностью «Компас Плюс», местонахождение: 455044, г. Магнитогорск, пр. Ленина, 68;
- Общество с ограниченной ответственностью «Рокет», местонахождение: 127055, г. Москва, ул. Сущевская д.27 с 2;
- Общество с ограниченной ответственностью «Лоялти Партнерс Восток», местонахождение: 105318, г. Москва, площадь Семеновская, 1А;
- Публичное акционерное общество «Европлан», местонахождение: 115093, г. Москва, 1-й Щипковский переулок, д.20;
- Общество с ограниченной ответственностью «Солид Дистрибьютор», местонахождение: 123007, г. Москва, Хорошевское шоссе, д.32А;

- Общество с ограниченной ответственностью «Юридическая Фирма «Адванс», местонахождение: 141400, Московская область, г. Химки, ул. Энгельса, 27, оф. 19;
- Акционерное общество «Город Денег», местонахождение: 115035, г. Москва, ул. Садовническая, д. 73, стр.1;
- АО «Национальное бюро кредитных историй», местонахождение: 121069, г. Москва, Скатертный пер., д. 20, стр. 1;
- Закрытое акционерное общество «Производственная фирма «СКБ Контур», местонахождения: 620017, г. Екатеринбург, пр. Космонавтов, д. 56;
- Общество с ограниченной ответственностью «АСТРАЛ-М», местонахождение: 111123 г. Москва, ул. Шоссе Энтузиастов, д.56, стр.32, офис 209;
- Акционерное общество «Оператор Финансовой Площадки», местонахождение: 119049, г. Москва, 4-й Добрынинский пер., д. 8;
- ООО "ЗЕТТА СТРАХОВАНИЕ", местонахождение: 121087, г. Москва, проезд Багратионовский, д. 7, оф. 11;
- АО "ТИНЬКОФФ БАНК", местонахождение: 123060, г. Москва, проезд Волоколамский 1-й, д. 10, оф. 1;
- ООО "КУБИК", местонахождение: 125171, г. Москва, ш. Ленинградское, д. 16а, стр. 3;
- Публичное Акционерное Общество "Росгосстрах", местонахождение: 140002, Московская область, г. Люберцы, ул. Парковая, д. 3;
- Общество с ограниченной ответственностью "СМАРТЛАЙН", местонахождение: 115280, г. Москва, ул. Ленинская Слобода, д. 19, корп. 21Е1;
- АО "Страховая Компания Опора", местонахождение: 111033, г. Москва, ул. Золоторожский вал, д. 11, стр. 29;
- Акционерное Общество "КОМПАНИЯ ОБЪЕДИНЕННЫХ КРЕДИТНЫХ КАРТОЧЕК", местонахождение: г. Москва, ул. Новочерёмушкинская, д. 10;
- Общество с ограниченной ответственностью "АТМ АЛЬЯНС", г. Москва, ул. Пятницкая, д. 37, оф. 2;
- РНКО «Платежный Центр» (ООО), местонахождение: г. Новосибирск, ул. Шатурская, д. 2;
- ООО "Платежный", местонахождение: г. Москва, ул. Покровка, д. 1 корп. 13 стр. 6;
- ООО "Современные Юридические Решения", местонахождение: г. Москва, ул. Электрозаводская, д. 24;
- Общество с ограниченной ответственностью "ВС-Экспресс", местонахождение: г. Москва, ул. Расплетина, д. 12 корп. 1;
- Общество с ограниченной ответственностью "Альфа Консалтинг", местонахождение: г. Омск, Челюскинцев, д. 85, кв. 10;
- Общество с ограниченной ответственностью "НОВЫЕ СИСТЕМЫ", местонахождение: 105082, г. Москва, ул. Бакунинская 69, стр. 1;
- ООО «СМС Трафик», местонахождение: 115088, Москва, 2-й Южнопортовый проезд, д.20А, стр.4, подъезд №1;
- ООО "МФМ СОЛЮШНС", местонахождение: 115280, Москва, ул. Ленинская Слобода, 19;
- УАНТУТРИП ТРЭВЕЛ ЭДЖЕНСИ ЛЛП / ONETWOTRIP Travel Agency LLP, местонахождение: Соединенное Королевство Великобритании и Северной Ирландии, Лейден Стрит 19, Лондон Е1 7LE 19;
- ООО «Мое дело», местонахождение: 105066, г. Москва, ул. Нижняя Красносельская, д. 39, стр. 3;

- АО «Лаборатория Касперского», местонахождение: 125212, Москва, шоссе Ленинградское, д. 39А;
- ООО «Логнекс», местонахождение: 117393, г. Москва, ул. Академика Пилюгина, д. 8, корп. 2;
- Общество с ограниченной ответственностью "Финансовые Сервисы Для Бизнеса", местонахождение: 119634, г.Москва, ул. Чоботовская, д. 17, пом. I, ком. 2;
- ООО «1С-Битрикс», местонахождение: 127287, г. Москва, ул. 2-я Хуторская, д. 38А, стр. 9;
- ООО «Кнопка», местонахождение: 143026, г. Москва, территория инновационного центра «Сколково», ул. Малевича, д. 1, пом. 6;
- КИВИ Банк (акционерное общество), местонахождение: 117648, г. Москва, мкр. Чертаново Северное, д. 1А, корп. 1;
- ООО «Деловая сфера», местонахождение: 109147, г. Москва, ул. Марксистская, д. 20, стр. 8;
- ООО «ФрииЭтЛаст», местонахождение: 123056, г. Москва, ул. Красина, д. 13;
- ООО «Бизнес элемент», местонахождение: 129344, г. Москва, ул. Искры, д. 31, корп. 1, ком. 15а, пом. III;
- ООО «БСС», местонахождение: 117105, г. Москва, проезд Нагорный, д. 5;
- Общество с ограниченной ответственностью «Открытие факторинг», местонахождение: 115432, г. Москва, проспект Андропова, д. 18, корпус 6, помещение 4-07;
- Общество с ограниченной ответственностью «СМ», местонахождение: 119607, г. Москва, проспект Мичуринский, 45;
- Общество с ограниченной ответственностью «КИВИ Процессинг», местонахождение: 141982, Московская область, г. Дубна, ул. Университетская, д. 7/2, помещение 22;
- ООО НПФ «Форус», местонахождение: 664011, Иркутская обл., г. Иркутск, ул. Свердлова, д. 41, оф. 1;
- ООО «Софтехно», местонахождение: 121552, г. Москва, ул. Ярцевская, д. 34, стр.1;
- ООО «Росгосстрах», местонахождение: 140002, Московская обл., г. Люберцы, ул. Парковая, д. 3;
- АО «АИГ», местонахождение: 125315, г. Москва, проспект Ленинградский, д. 72, корп. 2;
- ООО «АДМ КЛАУД», местонахождение: 123100, г. Москва, ул. 1905 года, д. 5, стр.1;
- Общество с ограниченной ответственностью «Хоум Кредит энд Финанс Банк», местонахождение: 125040, г. Москва, ул. Правды, д. 8, корп. 1;
- Общество с ограниченной ответственностью «Европейская Юридическая Служба», местонахождение: 121087, г. Москва, Багратионовский проезд, д.7, кор.20 В, офис 317;
- ООО «Лорес Консалтинг», местонахождение: 115054, г. Москва, ул. Дубининская, д.57, стр. 6, этаж/ком. 2/2;
- ПАО «Авиакомпания «Сибирь», местонахождение: 633104, Новосибирская обл., г. Обь, проспект Мозжерина, д. 10, оф. 201;
- Общество с ограниченной ответственностью «Инфосекьюрити Сервис», местонахождение: 119146, г. Москва, пр. Комсомольский, д. 7, стр. 2;
- ООО НКО «Яндекс.Деньги», местонахождение: 115035, г. Москва, ул. Садовническая, д. 82, стр. 2;

- ПАО Банк «ФК Открытие», 117216, Москва, ул. Старокачаловская 1, корпус 2;
- Публичное акционерное общество "МТС-Банк", местонахождение: 15432, г. Москва, проспект Андропова, д 18, корп. 1.

Согласие действует до момента получения Банком письменного заявления Клиента об отзыве настоящего согласия на обработку его персональных данных, но не более 50 лет.

3. По неурегулированным настоящими Правилами вопросам Стороны руководствуются действующим законодательством РФ.

4. Реквизиты Оператора:

Полное фирменное наименование: Акционерное общество «Точка»
Сокращенное фирменное наименование: АО «Точка»
ИНН /КПП 9705120864/770501001
ОГРН 1187746637143
Юридический адрес:109240, г.Москва, ул.Радищевская верхн., д.2/1, строение 5, пом.1, эт.3, ком.4
Адрес для направления корреспонденции: 620014, город Екатеринбург, улица Сакко и Ванцетти, дом 61
Название банка-получателя Филиал Точка Публичного акционерного общества Банка «Финансовая Корпорация Открытие»
Расчётный счёт 40702810202500015826
Корреспондентский счёт 30101810845250000999 в ГУ банка России по ЦФО
БИК банка 044525999
ИНН банка 7706092528
Сайт: www.tochka.com Телефон 8-800-2000-024

Приложение № 1

к Правилам дистанционного обслуживания в АО «Точка»

Заявление о присоединении к Правилам дистанционного обслуживания

Акционерного общества «Точка»

Я, _____, дата рождения _____,

1. Настоящим подтверждаю, что полностью и безоговорочно присоединяюсь к Правилам дистанционного обслуживания АО «Точка» (далее – Правила) условия которых определены АО «Точка» (далее - Оператор) и опубликованы на сайте https://tochka.com/, обязуюсь следовать положениям Правил, которые мне разъяснены и понятны в полном объеме.

2. Прошу использовать Электронную подпись, полученную мной в результате заключения Договора в соответствии с п. 2.5. Правил, в целях заключения сделок, получения услуг, оказываемых Оператором и/или Банками-партнерами.

3. Я даю свое согласие Оператору на осуществление моего фотографирования и/или аудио-/видеозаписи с моим участием и подтверждаю возможность дальнейшего использования полученных фотографии и/или аудио-/видеозаписи, в том числе, в качестве доказательств при рассмотрении споров компетентными органами.

4. Я признаю, что любая информация, подписанная моей электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному моей собственноручной подписью, и соответственно, порождает идентичные такому документу юридические последствия. Я оповещен(а) и соглашаюсь с предусмотренными Правилами моей обязанностью соблюдать конфиденциальность ключа электронной подписи и правилами определения лица, подписывающего электронный документ, проинформирован(а), о рисках, связанных с использованием электронной подписи.

5. В соответствии с требованиями Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных») настоящим даю свое согласие на обработку следующих персональных данных: фамилия, имя, отчество, пол, гражданство, дата и место рождения, данные документа, удостоверяющего личность, адрес, идентификационный номер налогоплательщика, страховой номер индивидуального лицевого счета, контактные данные (телефонный (абонентский) номер, адрес электронной почты), семейное, социальное, имущественное, финансовое положение, образование, профессия, доходы, биометрические персональные данные (в т.ч. фото-, видеоизображение, голос) и любая иная информация, относящаяся к моей личности, предоставленная мною для заключения Договора или в период его действия, а также полученная Оператором впоследствии для целей обеспечения соблюдения законов и иных нормативных правовых актов РФ, заключения, исполнения и обслуживания любых видов гражданско-правовых договоров, заключаемых между мной и Оператором, а также между Оператором и третьими лицами, в целях продвижения на рынке товаров, работ, услуг Оператора путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, для повышения и контроля за качеством обслуживания, а также в статистических целях.

Согласие дается как Оператору (Акционерному Обществу «Точка», ИНН 9705120864, место нахождения:109240, г. Москва, ул. Верхняя Радищевская дом 2/1, строение 5, пом. 1, этаж 3, ком. 4), так и любым третьим лицам, которые получили мои персональные данные, а также компаниям (в объеме фамилия, имя, отчество, адреса и номера телефонов), осуществляющим почтовую

рассылку по заявке Оператора. Перечень третьих лиц, в отношении которых даю согласие на обработку моих персональных данных, в целях продвижения услуг Оператора, совместных услуг Оператора и третьих лиц, продуктов (товаров, работ, услуг) третьих лиц, осуществления почтовых рассылок по заявке Банка приведен в Правилах.

Настоящее согласие предоставляется на осуществление любых действий в отношении моих персональных и биометрических персональных данных, которые необходимы для достижения указанных выше целей, совершаемые с использованием средств автоматизации или без использования таких средств: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Данное согласие действует с момента подписания настоящего Заявления до дня его отзыва (в письменной форме), но не более 50 лет. Я проинформирован(а), что лица, указанные в настоящем согласии, вправе после получения отзыва настоящего согласия, а равно после истечения срока действия настоящего согласия, продолжать обработку моих персональных данных при наличии оснований, предусмотренных частью 2 статьи 9 ФЗ «О персональных данных».
С объемом персональных данных, а также с перечнем третьих лиц, в отношении которых дается согласие на обработку моих персональных данных, указанных в Правилах, я ознакомлен(а) и согласен(на).

6. Действительность сведений подтверждаю.

Документ, удостоверяющий личность

_____

_____ _____ _____
серия номер дата выдачи

Номер телефона

+7_____

Прошу использовать данный Авторизованный номер для Дистанционного обслуживания.

Приложение № 2

к Правилам дистанционного обслуживания в АО «Точка»

1 Памятка по работе в Личном кабинете

1.1 В целях предотвратить хищение ЭП, Логина, Пароля, а также других реквизитов ЭП, необходимо придерживаться приведенных ниже правил и рекомендаций:

• Собственноручно задавая Пароль, ни в коем случае не пользоваться ключами, полученными от третьих лиц.

• Если выдача реквизитов ЭП происходила путем получения от Оператора смс-сообщения на телефон, удалить смс после прочтения.

• Использовать для хранения ЭП носители, к которым исключен доступ третьих лиц.

• На устройстве, с которого планируется осуществлять подключение в Личный кабинет, должны быть установлены лицензионные, регулярно обновляемые (устанавливаются обновления безопасности) операционная система, антивирусное программное обеспечение и web-браузер.

• На устройстве, с которого планируется осуществлять подключение в Личный кабинет, должен быть настроен и использоваться локальный межсетевой экран, настроенный на работу только с необходимыми сетевыми ресурсами по поддерживаемым ими протоколам.

• Устройство должно использовать процедуру аутентификации доступа к устройству прежде чем предоставить ресурсы пользователю (требуется ввод логина и пароля).

• При возникновении любых подозрений на компрометацию (копирование) ЭП или компрометацию среды исполнения (наличие в компьютере вредоносных программ) – обязательно позвонить Оператору и заблокировать ЭП.

• Отключать, извлекать носители с Ключами ЭП, если они не используются для работы в Личном кабинете.

• Ограничить доступ к компьютерам, используемым для работы в Личном кабинете. Исключить доступ к компьютерам персонала, не имеющего отношения к работе в Личном кабинете.

• На компьютерах, используемых для работы в Личном кабинете, исключить посещение интернет-сайтов сомнительного содержания, загрузку и установку нелицензионного ПО и т. п.

• Перейти к использованию лицензионного ПО (операционные системы, офисные пакеты и пр.), обеспечить автоматическое обновление системного и прикладного ПО.

• При обслуживании компьютера ИТ-сотрудниками – обеспечивать контроль за выполняемыми ими действиями.

• Не передавать ЭП ИТ-сотрудникам для проверки работы в Личном кабинете проверки настроек взаимодействия с Оператором и т.п. При необходимости таких проверок только лично владелец ЭП должен ее ввести, убедиться, что Пароль доступа вводится в интерфейс

клиентской системы Личный кабинет и лично ввести Пароль, исключая его подсматривание.

• При увольнении сотрудника, имевшего доступ к ЭП, обязательно позвонить Оператору и заблокировать ЭП.

• При увольнении ИТ-специалиста, осуществлявшего обслуживание компьютеров, используемых для работы с Личным кабинетом, принять меры для обеспечения отсутствия вредоносных программ на компьютерах.

• Если Вы заметили проявление необычного поведения ПО в Личном кабинете или какие-то изменения в интерфейсе программы – необходимо позвонить Оператору и выяснить, не связаны ли такие изменения с обновлением версии ПО. Если нет – необходимо заблокировать или сменить ЭП.

• Никогда и никому не сообщает Пароль, Логин и Одноразовые ключи/Цифровые коды (при их использовании).

• Клиент перед Аутентификацией входа должен убедиться, что в адресной строке браузера указан правильный адрес, указанный в Правилах.

• При использовании Одноразовых ключей: Клиент внимательно проверяет информацию об Операции, полученную в СМС-сообщений / Push-уведомлении с Одноразовым ключом на Операцию.

• Клиент убеждается, что используется защищенное SSL-соединение (отсутствуют сообщения об ошибке сертификата, в браузере изображен значок закрытого замка или рядом с адресной строкой имеется поле, индицирующее корректность SSL-соединения).

• Клиент, используя устройство, с которого получает доступ в Личный кабинет, осуществляет избирательную навигацию в сети Интернет и старается не посещать неизвестные ему сайты.

• Клиенту настоятельно не рекомендуется использование в качестве устройства доступа в Личный кабинет аппарата сотовой связи (сотового телефона, коммуникатора, смартфона, иного устройства), одновременно используемого для работы Авторизованного телефона Клиента и получения Одноразовых кодов (при их использовании).

• при любых подозрениях на мошеннические web-сайты, имитирующие Личный кабинет мошеннические СМС-сообщения/Push-уведомления или телефонные звонки, в которых неизвестные лица представляются как работники Оператора и/или Банка-партнера, Клиент обязан обратиться к Оператору по телефону, указанному на сайте в сети Интернет по адресу www.tochka.

• Важно понимать, что:

▫ Оператор не имеет доступа к Вашим ЭП, Паролям и не может от Вашего имени сформировать корректную ЭП под электронным платежным поручением.

▫ Вся ответственность за конфиденциальность Ваших ЭП, Паролей полностью лежит на Вас, как единственных владельцах ЭП.

▫ Оператор информирует Вас, что не осуществляет рассылку электронных писем с просьбой прислать ЭП или Пароль. Оператор не рассылает по электронной почте программы для установки на Ваши компьютеры.

▫ Если Вы сомневаетесь в конфиденциальности своих ЭП или есть подозрение в их компрометации (копировании), Вы должны заблокировать или сменить ЭП.

▫ Оператор настоящим еще раз информирует Вас о необходимости строгого соблюдения правил информационной безопасности, правил хранения и использования ЭП и о необходимости ограничения доступа к персональным компьютерам, с которых осуществляется работа в Личном кабинете.

▫ Действия злоумышленников направлены:

a) на похищение ЭП;

b) на похищение Пароля и/или Логина;

c) на передачу в Банк-партнер электронных расчетных документов, заверенных похищенной ЭП;

d) на подмену реквизитов получателя в платежном поручении, отправляемом Вами при работе в Личном кабинете.

2 Правила защиты от фишинга

2.1 Фишинг — это вид мошенничества, использующий сообщения электронной почты, и предназначенный для того, чтобы перенаправить пользователей на Web-сайты, разработанные специально для кражи банковских данных. Таким способом «фишеры» могут завладеть данными пользователя и использовать их в преступных целях. Они используют название и логотип Оператора, банка, чтобы завоевать доверие и совершить подлог. В фишинговом письме вам могут предложить так же пойти по ссылке на поддельный сайт или всплывающее окно, которые выглядит в точности так, как и оригинальный сайт, но созданные исключительно для целей похищения персональных данных. Еще при одном способе мошенничества вы все-таки попадете на настоящий сайт Оператора, но по пути вам загрузят шпионскую программу, которая будет передавать преступникам все, что вы наберете на клавиатуре. Доверчивые люди, обманутые такими мошенническими приемами, открывают злоумышленникам номера своих кредитных карт, Пароли и другую секретную информацию. Чтобы не попасть в такую ситуацию, крайне важно быть уверенным, что все транзакции совершаются в защищенной среде.

2.2 Как вам защитить себя:

2.2.1 Никогда не отвечайте на письма, запрашивающие вашу конфиденциальную информацию. Вы должны помнить, что мы никогда не будем связываться с вами по электронной почте, чтобы запросить какие-либо Пароли, данные Счетов, персональную информацию. Вам следует удалять любые полученные сообщения, запрашивающие личную информацию или содержащие ссылку на Web-страницу, где вам предлагается эти данные ввести. Вероятнее всего, такие сообщения являются мошенничеством.

2.2.2 Посетите Web-сайт Оператора путем ввода его URL-адреса через адресную строку браузера. Помните, что нельзя следовать ссылкам, указанным в письмах. Всегда вводите адреса через браузер.

2.2.3 Проверьте уровень защиты посещаемого вами сайта. Перед тем как ввести данные вашего Счета или другую конфиденциальную информацию, стоит провести несколько проверок, чтобы убедиться, что на Web-сайте для защиты ваших личных данных используются криптографические методы. Проверьте Web-адрес в адресной строке браузера. Если Web-сайт, который вы посетили, расположен на защищенном сервере, то адрес должен начинаться с «https://» («s» от security), а не с обычного «http://». Проверьте также состояние иконки с изображением замка в статусной строке вашего браузера. Вы можете проверить уровень криптозащиты, поводив курсором мыши над этой иконкой. Если остаются сомнения, убедитесь, что сертификат Web-страницы действителен, дважды щелкнув по замку.

2.2.4 Должны быть установлены лицензионные, регулярно обновляемые (устанавливаются обновления безопасности) операционная система, антивирусное программное обеспечение и web –браузер.

2.2.5 Всегда сообщайте об обнаруженной подозрительной активности. Если вы подозреваете, что получили поддельное электронное сообщение, перенаправьте его Оператору.

3 Памятка по использованию мобильных приложений

3.1 При потере Портативного устройства/смене номера телефона обязательно сообщите об этом Оператору.

3.2 Клиент должен использовать процедуру аутентификации доступа к Портативному устройству (ввод пароля для разблокировки Портативного устройства), прежде чем приступить к совершению операций через Мобильное приложение, если иной способ доступа не избран самим Клиентом.

3.3 Используйте только официальные приложения Оператора, доступные в официальных репозиториях производителей мобильных платформ.

3.4 Своевременно устанавливайте доступные обновления операционной системы и приложений на ваш телефон.

3.5 Портативное устройство не должно быть подвергнуто операциям повышения привилегий / взлома операционной системы устройства (jail-break, rooting).

3.6 Используйте антивирус для Портативного устройства, своевременно устанавливайте на него обновления вирусных баз.

3.7 Не переходите по ссылкам и не устанавливайте приложения/обновления безопасности, пришедшие по СМС/электронной почте, в том числе от имени Оператора или Банка-партнера.

3.8 Установите парольную защиту на Портативном устройстве, данная возможность доступна для любых современных Портативных устройств.

3.9 Установленный Цифровой код/ Touch ID код для входа в Мобильное приложение должен быть сложен для угадывания (отличаться от последовательности одинаковых символов, даты или года рождения Клиента и т.д.).

3.10 Клиент никогда и никому не должен сообщать Цифровой код/Touch ID код для входа в Мобильное приложение.

3.11 Клиент, используя Портативное устройство, с которого получает доступ к Мобильному приложению, осуществляет избирательную навигацию в сети Интернет, и старается не посещать неизвестные ему сайты, устанавливать сомнительные приложения.

3.12 Клиент обязуется не подключать Портативное устройство к компьютерам, безопасность которых (обеспечение доверенных сред, лишенных удаленного управления и установленных / запущенных вредоносных программ) он не может гарантировать.

3.13 Клиент обязуется не модифицировать или изменять Мобильное приложение, устанавливать приложение только из официальных хранилищ AppStore, Google Play и других.

3.14 Клиент понимает и подтверждает, что Оператору отправляются сведения о его геолокации.

3.15 Никогда не передавайте свое Портативное устройство и sim-карту третьим лицам.

3.16 Клиент, подключая опцию «совместная аналитика», дает поручение Оператору и Банку-партнеру передавать информацию об операциях по Счетам третьему лицу, указанному Клиентом при подключении вышеуказанной опции.

3.17 В случае если вы (Клиент) устанавливаете возможность просмотра информации в Системе «Точка» без ввода Цифрового кода, вы осознаете возможность реализации следующих рисков:

• В случае утери/кражи или выбытия Портативного устройства по иному основанию помимо воли Клиента, третьи лица могут получить доступ к следующей информации: о номере счета/счетов Клиента, об остатках и движении денежных средств по счету/счетам, наличии выпущенных Банковских карт, их количестве, номерах, сроке действия, действующим по Банковской карте лимитам, фамилии, имени, отчества владельца счета и держателя карты, наименование организации, которой принадлежит счет.

• В целях минимизации возможности реализации указанных в настоящем пункте рисков установите пароль для разблокировки Портативного устройства (в случае наличия технической возможности). В случае отсутствия такой возможности Оператор рекомендует не пользоваться услугой, позволяющей отменить Цифровой код для входа в Систему «Точка» с целью просмотра информации.

• Независимо от того, используете ли вы пароль для разблокировки Портативного устройства, риск возникновения негативных последствий, описанных в настоящем пункте, увеличивается в сравнении с тем, если бы вы постоянно использовали Цифровой код в Системе «Точка» для совершения любых действий, в том числе просмотра информации.

3.18 В случае установки Виджета Клиентом, использующим Мобильное приложение, Клиент осознает, что возможна реализация следующих рисков:

• В случае передачи Клиентом, утери/кражи или выбытия Портативного устройства по иному основанию помимо воли Клиента третьи лица могут получить доступ к следующей информации:

- текущий баланс Счета (-ов);

- о трех последних операциях, совершенных по Счету (-ам) Клиента;

В целях минимизации возможности реализации указанных в настоящем пункте рисков установите пароль для разблокировки Портативного устройства (в случае наличия технической возможности ограничения доступа к информации Виджета). В случае отсутствия такой возможности Оператор рекомендует не пользоваться вышеуказанной опцией.

Факт использования Виджета несет повышенный риск возникновения негативных последствий, описанных в настоящем пункте, в сравнении с тем, если бы Вы постоянно использовали исключительно Мобильное приложение для просмотра информации.

3.19 В случае использования Клиентом – пользователем Мобильного приложения, Портативного устройства, оснащенного технологией 3D Touch, Клиент осознает, что возможна реализация следующих рисков:

• В случае передачи Клиентом, утери/кражи или выбытия Портативного устройства по иному основанию помимо воли Клиента третьи лица могут получить доступ к следующей информации:

- о текущем балансе Счета(-ов);

В целях минимизации возможности реализации указанных в настоящем пункте рисков установите пароль для разблокировки Портативного устройства.

3.20 Подключение Личного кабинета, мобильных приложений либо иного электронного средства платежа является высокорискованным и не исключает вероятности использования электронного средства платежа без согласия Клиента.

3.21 Оператор и Банк-партнер не отвечают за убытки Клиента, возникшие в результате внесения Клиентом или третьими лицами изменений в программное обеспечение Портативного устройства, компьютера или иного устройства, обеспечивающего доступ в Мобильное приложение, а также в результате наличия «вирусов» и иных вредоносных программ в указанных устройствах и программном обеспечении, используемом Клиентом для доступа в Мобильное приложение.

3.22 Стороны признают используемые ими по Договору системы телекоммуникаций, обработки и хранения информации достаточными для обеспечения надежной и эффективной работы при приеме, передаче, обработке и хранении информации, а систему защиты информации, обеспечивающую разграничение доступа, шифрование, формирование и проверку подлинности средств доступа достаточной для защиты от несанкционированного доступа, подтверждения авторства и подлинности информации, содержащейся в получаемых электронных документах, и разбора конфликтных ситуаций.