

Приложение №11

к Договору комплексного банковского обслуживания юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, в ООО «Вайлдберриз Банк»

ПРАВИЛА ОКАЗАНИЯ УСЛУГ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ ЮРИДИЧЕСКИХ ЛИЦ, ИНДИВИДУАЛЬНЫХ ПРЕДПРИНИМАТЕЛЕЙ, ФИЗИЧЕСКИХ ЛИЦ, ЗАНИМАЮЩИХСЯ В УСТАНОВЛЕННОМ ЗАКОНОДАТЕЛЬСТВОМ РОССИЙСКОЙ ФЕДЕРАЦИИ ПОРЯДКЕ ЧАСТНОЙ ПРАКТИКОЙ, В СИСТЕМЕ FAKTURA.RU В ООО «ВАЙЛДБЕРРИЗ БАНК»

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Указанные в настоящих Правилах оказания услуг дистанционного банковского обслуживания юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, в системе Faktura.ru в ООО «Вайлдберриз Банк» (далее – Правила) термины и определения с прописной (заглавной) буквы применяются в определении, содержащемся в разделе «Термины и определения» Договора КБО, если иное прямо не оговорено в тексте настоящих Правил, за исключением следующих терминов, имеющих указанное ниже значение:

Банк – Общество с ограниченной ответственностью «Вайлдберриз Банк» (ООО «Вайлдберриз Банк»), лицензия Банка России № 841 от 06.08.2021.

Вредоносный код - компьютерная программа, предназначенная для внедрения в автоматизированные системы, программное обеспечение, средства вычислительной техники, телекоммуникационное оборудование Банка и/или Клиента, приводящего к уничтожению, созданию, копированию, блокированию, модификации и (или) передаче информации, а также к созданию условий для такого уничтожения, создания, копирования, блокирования, модификации и (или) передачи.

Клиент - юридическое лицо (за исключением кредитных организаций), иностранная структура без образования юридического лица, индивидуальный предприниматель или физическое лицо, занимающееся в установленном законодательством РФ порядке частной практикой.

Компрометация - утрата/хищение средства подтверждения, любые признаки осуществления несанкционированных действий в системе Faktura.ru, а также случаи, когда нельзя достоверно установить, что произошло со средством подтверждения, паролем.

Номер мобильного телефона – номер мобильного телефона Клиента, предоставленный Участнику Системы оператором сотовой связи и указанный Клиентом при регистрации Клиента в Системе (либо измененный Участником в установленном порядке).

Одноразовый пароль - динамическая аутентификационная информация, генерируемая для единичного использования.

Простая электронная подпись (далее – ПЭП) - электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

Разовый СМС-пароль – уникальный набор символов, используемый для подтверждения простого ЭД / группы простых ЭД, аутентификации клиента и совершения иных действий. Разовый СМС-пароль направляется Клиенту на Номер мобильного телефона путем направления СМС-сообщения/Push-сообщения. Разовый СМС-пароль имеет ограниченный срок действия, определяемый Системой.

Система Faktura.ru (далее – Система) - система дистанционного банковского обслуживания, включающая сервисы «Интернет-Банк» и «Мобильный банк» и представляющая собой совокупность программного, информационного и аппаратного обеспечения, реализующая электронный документооборот между Банком и Клиентом.

Сочетание подписей - комбинации ЭП лиц, наделенных правом подписи, необходимые для подписания ЭД, содержащих распоряжение Клиента (в соответствии соглашением между Банком и Клиентом и/или карточкой с образцами подписей и оттиском печати).

Средство подтверждения - электронное средство (мобильный телефон), используемое для подтверждения электронного документа одноразовыми паролями. Использование средств подтверждения является наиболее эффективной мерой защиты платежных документов от несанкционированного доступа в Систему посторонних лиц.

Участник Системы (Участник) – Клиент, а также уполномоченное должностное лицо Клиента, при их совместном упоминании.

Электронный документ (далее – ЭД) - информация, представленная в электронной форме, содержащая финансовый документ (платежное распоряжение) или распоряжение по подключению, отключению или изменению предоставляемых Банком услуг в рамках расчетно-кассового обслуживания, информационное сообщение в системе, заявления, учредительные документы, финансовая отчетность и иные документы в электронной форме, предоставляемые в Банк. Электронные документы хранятся в электронных системах Системы и/или Банка.

Электронная подпись (далее – ЭП) - информация в электронной форме, присоединенная к другой информации в электронной форме (подписываемой информации) или иным образом связанная с такой информацией, и используемая для определения лица, подписывающего информацию. Электронная подпись – неквалифицированная электронная подпись / квалифицированная электронная подпись / простая электронная подпись (НЭП/КЭП/ПЭП), как их определяет Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящие Правила оказания услуг дистанционного банковского обслуживания юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, в системе Faktura.ru в ООО «Вайлдберриз Банк» (далее – Правила) определяют условия и порядок использования Системы Участником, устанавливают порядок обмена документами между Клиентом и Банком, в которых информация представлена в электронной форме и заверена ПЭП с помощью Системы. С использованием Системы Банк оказывает Клиенту услуги по дистанционному банковскому обслуживанию Счета(-ов) Клиента, открытого(-ых) в Банке, а также по обмену электронными документами между Клиентом и Банком.

2.2. Обязательным условием подключения Клиента к Системе является наличие у Клиента, открытого в Банке расчетного счета.

2.3. Электронный документооборот по обмену ЭД между Банком и Клиентом осуществляется в порядке и на условиях, определенных Правилами электронного документооборота Корпоративной Информационной Системы «BeSafe» компании «Центр Финансовых Технологий», расположенных на веб-сервере по адресу: <http://www.besafe.ru>.

2.4. Информационный обмен в рамках Системы осуществляется по открытым каналам связи, в том числе с использованием сети Интернет.

2.5. Для обеспечения конфиденциальности ЭД при его передаче по открытым каналам связи, а также для обеспечения авторства и целостности ЭД в Системе используются программные средства защиты информации, реализующие алгоритмы шифрования, формирования и проверки ЭП.

2.6. На основании настоящих Правил с использованием Системы осуществляется обмен следующими ЭД:

- распоряжение о переводе денежных средств со счета в рублях/иностранной валюте, открытом Клиенту в Банке;
- документы и информация, которые связаны с проведением валютных операций;
- информационные письма Клиентов с приложенными к ним файлами, хранящиеся в виде записи в контрольных архивах Системы или извлеченные из нее в виде отдельного файла.

Вышеуказанный перечень ЭД может изменяться Банком в одностороннем порядке с последующим информированием Клиента.

Направление Клиентом Банку иных видов ЭД может осуществляться после предварительного согласования с Банком. Согласием Банка является, в т.ч. принятие электронного документа, содержащегося в письме, к исполнению.

2.7. В целях реализации настоящих Правил Система является электронным средством платежа - средством, позволяющим Клиенту Банка составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации.

2.8. Клиентская часть Системы может быть представлена Клиенту в виде доступа к Web-серверу «Faktura.ru» или в виде мобильного приложения для мобильного устройства на базе Android и iOS.

2.9. При работе в Системе Клиент использует одновременно и логин, и пароль.

3. УСЛОВИЯ РАБОТЫ В СИСТЕМЕ

3.1. Подключение к Системе производится при наличии у Клиента доступа к сети Интернет, обеспечиваемого Клиентом, и собственного комплекта технического оборудования, удовлетворяющего требованиям Системы.

3.2. Регистрация Участника в Системе для оказания Банком услуг в рамках настоящих Правил осуществляется на основании Заявления о присоединении к ДКБО Клиента, оформленного по форме Банка.

3.3. Участниками системы могут быть только уполномоченные должностные лица Клиента, в отношении которых Банком проведена идентификация и установлены их полномочия.

3.4. Банк на основании Заявления Клиента производит генерацию логина и одноразового пароля и направляет их отдельными СМС-сообщениями на номер мобильного телефона Участника, указанный в Заявлении Клиента.

3.5. Одноразовый пароль является временным и должен быть изменён Участником самостоятельно при первом входе в Систему. Срок действия одноразового пароля – 14 (четырнадцать) календарных дней. Вход в Систему возможен только при выполнении условия смены одноразового пароля на постоянный пароль при первом входе.

Банк при этом не несет ответственности за доставку СМС-сообщения Клиенту по причине возможных сбоев у мобильных операторов и в самой Системе. В случае неполучения СМС-сообщения с логином и/или одноразовым паролем в течение 2 (Двух) рабочих дней с момента заключения Договора/подключения услуги, Клиент должен лично обратиться в Банк.

3.6. Начало работы уполномоченного должностного лица Клиента в Системе осуществляется посредством ввода его логина и пароля в Систему.

3.7. Изменение в составе уполномоченных должностных лиц Клиента и/или номеров телефона уполномоченных должностных лиц Клиента осуществляется посредством личного обращения единоличного исполнительного органа Клиента (индивидуального предпринимателя) с соответствующим заявлением в подразделение Банка по форме Приложения № 11.1 к настоящим Правилам (далее – Заявление). Также Заявление, подписанное ЭП Клиента/Представителя Клиента может быть направлено по Системе или Заявление, подписанное аналогом собственноручной подписи Клиента/Представителя Клиента, усиленной квалифицированной электронной подписью, создаваемой при помощи криптографического кода, может быть направлено по электронной почте.

3.8. Исполнение заявления о прекращении полномочий/изменение номера телефона уполномоченного должностного лица Клиента осуществляется в течение 1 (одного) рабочего дня с момента получения Банком такого заявления.

3.9. Исполнение заявления о включении в состав уполномоченных должностных лиц Клиента нового лица, а также изменение номера телефона действующего уполномоченного должностного лица Клиента, осуществляется посредством процедуры регистрации данного лица в Системе в порядке, установленным пп. 3.2. - 3.8. настоящих Правил.

3.10. При входе (идентификации и аутентификации) в Систему Клиент использует ПЭП в виде Логин/Пароль/SMS для подписи всех электронных документов, отправляемых в Банк.

3.11. Клиент, при работе с Системой, принимает на себя следующие обязательства, связанные с информационной безопасностью:

- использовать в работе только лицензионные версии операционных систем и прикладного программного обеспечения;
- применять и своевременно обновлять средства антивирусной защиты;
- своевременно устанавливать обновления безопасности для используемого программного обеспечения, в том числе мобильных приложений;
- не передавать логин/пароль/SMS третьим лицам, обеспечить сохранность указанных сведений;
- не использовать неизвестные/сомнительные Wi-Fi сети для подключения к сети Интернет;
- не передавать мобильное устройство, которое используется в качестве рабочего места для работы в Системе/ получения SMS, либо Средство подтверждения третьим лицам;
- активировать на мобильном устройстве, либо на Средстве подтверждения встроенное средство безопасности – пин-код, графический рисунок, отпечаток пальца либо фейс-айди.
- обеспечить непрерывное нахождение мобильного устройства под контролем уполномоченного лица Клиента.

3.12. Запрещается использование Системы в следующих случаях (включая, но не ограничиваясь):

- Клиентом не выполнены организационные меры для обеспечения безопасной работы в Системе;
- Клиент не обеспечил надежное хранение и защиту от компрометации средств, использующихся для дистанционного распоряжения счетом Клиента. К указанным средствам относятся мобильное

устройство, логин, пароль, зарегистрированный в Системе номер мобильного телефона, Средство подтверждения.

- Клиентом не обеспечен запрет использования на рабочем месте средств удаленного управления (R-Admin, TeamViewer и аналоги), администрирования и модификации ОС и её настроек (службы терминалов, удаленных рабочих столов и аналоги);

- Клиент не настроил канал оповещения о совершенных операциях (для мобильных приложений).

3.13. Клиент уведомлен и согласен, что при использовании Системы он несет повышенные риски, связанные с несанкционированным списанием средств Клиента неуполномоченными лицами, в том числе и с использованием Вредоносного кода. Начиная работать с Системой, Клиент подтверждает, что он полностью принимает на себя указанные риски.

3.14. Клиент несет полную ответственность за действия, совершенные третьими лицами, в случае передачи Клиентом средств, использующихся для дистанционного распоряжения счетом Клиента указанным лицам и/или в случае создания Клиентом условий для несанкционированного использования третьими лицами средств, использующихся для дистанционного распоряжения счетом Клиента. Клиент также несет полную ответственность за ущерб, причиненный Банку, указанными действиями или бездействием.

3.15. Клиент согласен с использованием логов (журналов) Системы и журналов модуля Системы по детектированию вредоносного программного обеспечения в качестве доказательства при разбирательстве по факту нарушений настоящих Правил и организационных мер для обеспечения безопасной работы в Системе.

4. СОГЛАШЕНИЯ СТОРОН

4.1. Для подписания ЭД стороны используют ПЭП. Стороны признают, что применяемая в Системе защита информации, обеспечивающая шифрование, контроль целостности и создание ПЭП, достаточна для защиты информации от несанкционированного доступа, подтверждения подлинности и авторства ЭД.

4.2. Клиент (представитель Клиента), создающий электронный документ в Системе и подписывающий такой электронный документ ПЭП, определяется как лицо, авторизованное и идентифицированное Системой.

4.3. При работе в Системе разовый СМС-пароль генерируется Системой в момент подтверждения Клиентом факта отправки документа в Банк и отправляется Клиенту посредством СМС-сообщения на номер мобильного телефона Клиента, указанный в Заявлении.

4.4. Электронные документы, подтвержденные ПЭП, считаются переданными Клиентом, и в случае доставки их в Банк, полученными Банком, а соответствующая операция подлежит исполнению и выполняется Банком от имени и по поручению Клиента, если Системой подтверждена передача.

4.5. Стороны договорились считать, что Клиент отказался от передачи электронного документа до его отправки в Банк, если он не подтвердил правильность ввода информации ПЭП.

4.6. Электронные документы, заверенные ПЭП Клиента, юридически эквивалентны соответствующим документам на бумажном носителе, подписанным лицом, которому предоставлено право распоряжаться денежными средствами на счете Клиента и имеющим отпечаток печати Клиента (при наличии), обладают юридической силой и подтверждают наличие правовых отношений между Сторонами. Электронные документы без ПЭП Клиента не имеют юридической силы, Банком не рассматриваются и не исполняются.

4.7. Электронные документы с ПЭП Клиента, создаваемые Клиентом в Системе и полученные Банком, являются доказательным материалом для решения спорных вопросов в соответствии с «Положением о процедуре разбора конфликтной ситуации в рамках использования системы Faktura.ru» в ООО Вайлдберриз Банк» (Приложение № 11.2 к Правилам).

4.8. По заявлению Клиента в Системе могут быть установлены ежедневные лимиты на проведение операций по Системе. Заявление составляется по форме Приложения № 11.3 к Правилам.

4.9. Стороны признают в качестве единой шкалы времени при работе с Системой московское поясное время. Контрольным является время системных часов Системы.

4.10. Стороны признают, что подделка одноразового пароля, то есть подтверждение ЭД от имени Клиента, невозможна без владения соответствующим Средством подтверждения.

4.11. Стороны признают, что ЭД должны быть подписаны ПЭП уполномоченных лиц в сочетании, определенном соответствующим соглашением между Клиентом и Банком.

4.12. Стороны признают, что возможность воспроизведения в электронном виде и на бумажных носителях принятого к исполнению и исполненного Банком платежного распоряжения Клиента с отметками Банка осуществляется с использованием Системы. Получение платежного распоряжения на бумажном носителе с отметками Банка может осуществляться также в офисе Банка по месту обслуживания счета Клиента в соответствии с графиком работы Банка.

4.13. Банк осуществляет информирование Клиента о совершенных операциях посредством направления уведомлений одним из способов:

4.13.1. Путем отправки СМС-сообщения/ Push-сообщений на номер мобильного телефона Участника, указанный Клиентом в Заявлении. Обязанность банка по информированию Клиента считается исполненной Банком с момента отправки Банком СМС-сообщения/Push-сообщений на номер мобильного телефона Клиента. Банк не несет ответственности в случае несвоевременного уведомления Банка Клиентом об изменении номеров телефонов, в том числе используемых для получения СМС-сообщений/Push-сообщений, а также за действия или бездействие третьих лиц, влияющих на время и возможность получения Клиентом уведомлений от Банка о совершении операции по счету Клиента.

4.13.2. Путем изменения статуса соответствующего электронного документа в Системе. Присвоение электронному документу в Системе статуса «Отправлен в банк» подтверждает, что документ отправлен в Банк, но еще не получен. Присвоение электронному документу в Системе статуса «Принят Банком» подтверждает прием Банком распоряжения Клиента к исполнению. Присвоение электронному документу статуса «Исполнен» подтверждает исполнение Банком распоряжения Клиента. Присвоение электронному документу статуса «В картотеке» подтверждает помещение распоряжения в картотеку документов Клиента. Присвоение электронному документу статуса «Возвращен» подтверждает аннулирование Банком распоряжения Клиента. Уведомление считается полученным Клиентом с момента изменения статуса ЭД в Системе.

4.13.3. Путем направления выписки по банковскому счету Клиента. Уведомление считается полученным Клиентом с момента отправки Банком выписки в Систему.

4.13.4. Банк обязан проинформировать Клиента о совершенных операциях в Системе не позднее дня, следующего за днем исполнения соответствующей операции.

4.14. Стороны признают надлежащим уведомление Клиента о совершенных операциях в Системе способами, указанными в п. 4.13. настоящих Правил.

5. ПРАВА И ОБЯЗАННОСТИ КЛИЕНТА

5.1. Клиент вправе:

5.1.1. В любой момент прекратить действие Средства подтверждения, оформив уведомление по форме Приложения № 11.4 к настоящим Правилам.

5.1.2. Приостановить/прекратить использовать Систему Faktura.ru оформив уведомление по форме Приложения № 11.4 к настоящим Правилам.

5.1.3. Клиент имеет право обращаться за получением консультаций, связанных с обслуживанием Клиента, а также эксплуатацией Системы.

5.2. Клиент обязан:

5.2.1. Использовать только лицензионные операционные системы, поддерживаемые компанией производителем, для работы в Системе.

5.2.2. Обеспечивать информационную безопасность рабочих мест и мобильных устройств ответственных сотрудников, уполномоченных использовать Систему для взаимодействия с Банком. Клиент обязан исключить или максимально ограничить доступ к этим рабочим местам лиц, чья деятельность не связана с осуществлением электронного документооборота с Банком.

5.2.3. Ознакомиться с описанием механизмов защиты Системы и требованиями по обеспечению информационной безопасности своего рабочего места и соблюдать их (Приложение № 11.5 к Правилам).

5.2.4. Заполнять ЭД в Системе в соответствии с требованиями действующего законодательства РФ.

5.2.5. Хранить в секрете логин и пароль, не предоставлять непосредственный или удаленный доступ к Средству подтверждения, используемому в Системе, а также обеспечить их защиту от использования третьими лицами.

5.2.6. Обеспечивать использование логина, пароля, СМС-сообщения/Push-сообщения только их владельцами (уполномоченными должностными лицами) в соответствии с установленными правами подписи.

5.2.7. По требованию Банка прекратить использование указанного логина и пароля или сменить пароль.

5.2.8. Предоставить Банку достоверную и актуальную информацию для связи с уполномоченными должностными лицами Клиента.

5.2.9. В случае изменения информации для связи своевременно предоставить Банку обновленную информацию. Обязанность Банка по направлению Клиенту уведомлений считается исполненной при направлении уведомления в соответствии с имеющейся у Банка информацией для связи.

5.2.10. В случае компрометации логина/пароля или Средства подтверждения Клиент обязан незамедлительно проинформировать Банк путем направления соответствующего сообщения на эл. адрес: feedback@wb-bank.ru или по телефону: +7(495)600-37-61.

5.2.11. Исполнять обязательства, возникшие до момента приостановления или прекращения использования Клиентом Системы.

5.2.12. Незамедлительно уведомить Банк о прекращении/изменении полномочий лиц, имеющих учетные записи в Системе, но в любом случае не позднее 5 (Пяти) рабочих дней с даты прекращения/изменения полномочий. Клиент несет полную ответственность за неблагоприятные последствия, связанные с получением информации по счетам Клиента, а также созданием и подписью ЭД такими лицами после прекращения/изменения их полномочий.

6. БЛОКИРОВКА/РАЗБЛОКИРОВКА СИСТЕМЫ

6.1. Блокировка Системы представляет собой процедуру установления ограничений на совершение операций в Системе.

6.2. По инициативе Клиента Банк производит блокировку Системы в следующих случаях:

- в случаях компрометации личного кабинета Системы;
- в иных случаях по усмотрению Клиента.

6.3. Блокировка Системы по инициативе Клиента осуществляется после успешного прохождения Клиентом Авторизации/Аутентификации на основании запроса на блокировку, оформленного Клиентом через каналы Системы, Службу поддержки.

6.4. Разблокировка Системы по инициативе Клиента осуществляется после успешного прохождения Клиентом Авторизации.

Разблокировка Системы осуществляется Банком по истечении 24 часов с момента ее блокировки, если в Банк не поступит от Клиента заявление о совершении операции без его добровольного согласия.

Разблокировка Системы осуществляется Клиентом самостоятельно путем повторной Авторизации с использованием приложения мобильного банка.

6.5. Банк вправе в одностороннем порядке заблокировать доступ к каналам Системы или ограничить Клиента в использовании Системы (для совершения операций) до выяснения причин, в следующих случаях:

- при наличии у Банка подозрений компрометации Системы;
- в случае нарушения Клиентом условий ДКБО и настоящих Правил или предоставления Банку недостоверной информации;
- при наличии у Банка информации о вероятных или действительных противозаконных операциях или операциях, которые могут повлечь за собой ущерб для Банка или Клиента;
- в случае наличия нестандартных или необычно сложных схем проведения операций, отличающихся от обычного порядка операций, характерных для клиентов, пользующихся Системой;
- при выполнении Банком требований Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее - Федеральный закон № 115-ФЗ), Федерального закона от 10.12.2003 № 173-ФЗ «О валютном регулировании и валютном контроле» (далее - Федеральный закон № 173-ФЗ), Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» (далее - Федеральный закон № 161-ФЗ); Федерального закона от 26.10.2002 № 127-ФЗ «О несостоятельности (банкротстве)» (далее - Федеральный закон № 127-ФЗ);
- в иных случаях, предусмотренных законодательством Российской Федерации и нормативными правовыми актами.

6.6. Банк информирует Клиента о блокировке доступа к Системе с указанием причин блокировки в день установления такой блокировки путем размещения информации в приложении мобильного банка и/или путем направления Клиенту Push-уведомления.

6.7. В случае блокировки доступа в Систему по инициативе Банка установлены следующие сроки блокирования в зависимости от основания блокирования:

- до момента полного устранения Клиентом допущенных им нарушений порядка использования Системы;
- до момента рассмотрения Банком, предоставленных Клиентом разъяснений и документов о совершаемой операции, затребованных Банком;
- до момента принятия Банком решения по последствиям выявленных фактов несанкционированного доступа, но не более 3 (Трех) месяцев с даты блокирования Системы;
- либо на срок, установленный законодательством Российской Федерации и нормативными правовыми актами.

6.8. Заблокированные по решению Банка, доступ в Системы могут быть разблокированы по инициативе Банка, после устранения нарушений порядка использования Системы или иных обстоятельств, повлекших блокировку.

6.9. В случае выявления Банком операции, соответствующей установленным Банком России признакам осуществления перевода денежных средств без добровольного согласия Клиента, а именно без согласия Клиента или с согласия Клиента, полученного под влиянием обмана или при злоупотреблении доверием (далее при совместном упоминании - перевод денежных средств без добровольного согласия Клиента) до момента списания денежных средств, Банк приостанавливает прием к исполнению распоряжения о переводе денежных средств Клиента на 2 (два) дня и осуществляет блокировку доступа в Систему с уведомлением Клиента в день такой блокировки с указанием причины путем направления СМС-сообщения или Push-уведомления.

Банк обязан осуществить проверку наличия признаков осуществления перевода денежных средств без добровольного согласия Клиента, до момента списания денежных средств Клиента (за исключением операции с использованием платежных карт, перевода электронных денежных средств или перевода денежных средств с использованием СБП) либо при приеме к исполнению распоряжения клиента (при осуществлении перевода денежных средств в иных случаях).

Проверка наличия признаков осуществления перевода денежных средств без добровольного согласия Клиента осуществляется с учетом информации, полученной от оператора по переводу денежных средств, обслуживающего получателя средств, при выявлении операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента, если это предусмотрено правилами платежной системы, в рамках которой осуществляется перевод денежных средств, оператору по переводу денежных средств, обслуживающему плательщика, о такой операции в рамках реализации мероприятий по противодействию осуществлению переводов денежных средств без добровольного согласия Клиента.

Банк при выявлении им операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента (за исключением операции с использованием платежных карт, перевода электронных денежных средств или перевода денежных средств с использованием СБП), приостанавливает прием к исполнению распоряжения Клиента на 2 (Два) дня и осуществляет блокировку доступа в Систему с уведомлением Клиента в день такой блокировки с указанием причины путем направления СМС-сообщения или Push-уведомления. Банк при выявлении им операции с использованием платежных карт, перевода электронных денежных средств или перевода денежных средств с использованием СБП, соответствующих признакам осуществления перевода денежных средств без добровольного согласия Клиента, отказывает в совершении соответствующей операции (перевода).

6.10. Банк информирует Клиента:

- о приостановлении исполнения распоряжения о совершении операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента;
- о рекомендациях по снижению рисков повторного осуществления перевода без добровольного согласия Клиента и незамедлительно запрашивает у Клиента подтверждение возобновления исполнения распоряжения;

- о возможности Клиента подтвердить распоряжение не позднее 1 (Одного) дня, следующего за днем приостановления Банком приема к исполнению указанного распоряжения, способами, предусмотренными настоящими Правилами или о возможности совершения Клиентом повторной операции, содержащей те же реквизиты получателя (плательщика) и ту же сумму перевода (далее – повторная операция), способами, предусмотренными настоящими Правилами, в случае отказа Банка в совершении Клиентом операции с использованием платежных карт, перевода электронных денежных средств или перевода денежных средств с использованием СБП платежной системы Банка России.

6.11. Банк при предоставлении Клиенту информации в соответствии с п. 5.10 настоящих Правил вправе в дополнение к подтверждению Клиента запросить у Клиента информацию, что перевод денежных средств не является переводом денежных средств без добровольного согласия Клиента, и (или) направить Клиенту информацию о необходимости совершить повторную операцию способом, который предусмотрен настоящими Правилами.

6.12. При получении от Клиента подтверждения распоряжения или осуществлении действий по совершению Клиентом повторной операции Банк обязан разблокировать доступ в Систему и незамедлительно принять к исполнению подтвержденное распоряжение Клиента или совершить повторную операцию, при отсутствии иных установленных законодательством Российской Федерации оснований не принимать распоряжение Клиента к исполнению.

6.13. При неполучении от Клиента подтверждения распоряжения и (или) запрошенной Банком информации, указанное распоряжение считается не принятым к исполнению, а при осуществлении

действий по совершению Клиентом повторной операции способом, не предусмотренным настоящими Правилами, повторная операция считается несовершенной.

6.14. В случае, если, несмотря на направление Клиентом подтверждения распоряжения или осуществление действий по совершению повторной операции, Банк получил от Банка России информацию, содержащуюся в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента, Банк приостанавливает прием к исполнению подтвержденного распоряжения Клиента на 2 (Два) дня со дня направления Клиентом подтверждения распоряжения или отказывает в совершении Клиентом повторной операции. Банк незамедлительно уведомляет Клиента о приостановлении приема к исполнению подтвержденного распоряжения Клиента или об отказе в совершении Клиентом повторной операции с указанием причины такого приостановления (отказа) и срока такого приостановления, а также о возможности совершения Клиентом последующей повторной операции.

6.15. В случае приостановления приема к исполнению подтвержденного распоряжения Клиента в соответствии с п. 6.14 настоящих Правил по истечении 2 (Двух) дней со дня направления Клиентом подтверждения распоряжения Банк обязан незамедлительно принять к исполнению подтвержденное распоряжение Клиента при отсутствии иных установленных законодательством Российской Федерации оснований не принимать подтвержденное распоряжение Клиента к исполнению. В случае отказа в совершении Клиентом повторной операции по истечении 2 (Двух) дней со дня осуществления действий по совершению Клиентом повторной операции Банк обязан совершить последующую повторную операцию Клиента при отсутствии иных установленных законодательством Российской Федерации оснований не совершать последующую повторную операцию Клиента.

6.16. В случае, если Банк получил от Банка России информацию, содержащуюся в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента, и после получения от Банка России указанной информации исполняет распоряжение Клиента об осуществлении перевода денежных средств или совершает операцию с использованием платежных карт, перевод электронных денежных средств или перевод денежных средств с использованием СБП, соответствующие признакам осуществления перевода денежных средств без добровольного согласия Клиента, Банк обязан возместить Клиенту сумму перевода денежных средств или операции с использованием платежных карт, перевода электронных денежных средств или перевода денежных средств с использованием СБП без добровольного согласия Клиента в течение 30 (тридцати) дней, следующих за днем получения соответствующего заявления Клиента.

6.17. В случае, если Банк получил от Банка России информацию, содержащуюся в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента, которая содержит сведения, относящиеся к Клиенту и (или) его электронному средству платежа (далее – ЭСП), и если отсутствуют сведения федерального органа исполнительной власти в сфере внутренних дел о совершенных противоправных действиях, получаемые Банком в соответствии с Федеральным законом от 27.06.2011 № 161-ФЗ, Банк в рамках реализуемой им системы управления рисками и в порядке, предусмотренном настоящими Правилами, вправе приостановить использование Клиентом ЭСП на период нахождения сведений, относящихся к Клиенту и (или) его ЭСП, в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента. В случае, если использование Клиентом ЭСП не было приостановлено в соответствии с настоящей частью Правил, в период нахождения сведений, относящихся к Клиенту и (или) его ЭСП, в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента Банк осуществляет переводы денежных средств с использованием ЭСП по распоряжению Клиента - физического лица в пользу получателей - физических лиц на сумму не более 100 тысяч рублей в месяц.

6.18. Банк обязан приостановить использование Клиентом ЭСП, если от Банка России получена информация, содержащаяся в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента, которая содержит сведения, относящиеся к Клиенту и (или) его ЭСП, в том числе сведения федерального органа исполнительной власти в сфере внутренних дел о совершенных противоправных действиях, на период нахождения указанных сведений в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента.

6.19. После приостановления использования Клиентом ЭСП Банк незамедлительно уведомляет Клиента о приостановлении использования ЭСП, а также о праве Клиента подать в порядке, установленном Банком России, заявление в Банк России, в том числе через Банк, об исключении сведений, относящихся к Клиенту и (или) его ЭСП, в том числе сведений федерального органа исполнительной власти в сфере внутренних дел о совершенных противоправных действиях, из базы данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента.

6.20. В случае наличия у Банка оснований полагать, что включение сведений, относящихся к Клиенту и (или) его ЭСП, в базу данных о случаях и попытках осуществления переводов денежных

средств без добровольного согласия Клиента является необоснованным, Банк вправе самостоятельно (без участия Клиента) направить в Банк России мотивированное заявление об исключении сведений, относящихся к Клиенту и (или) его ЭСП, в том числе сведений федерального органа исполнительной власти в сфере внутренних дел о совершенных противоправных действиях, из базы данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента.

6.21. В случае получения в порядке, установленном Банком России, информации об исключении сведений, относящихся к Клиенту и (или) его ЭСП, из базы данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента Банк незамедлительно возобновляет исполнение распоряжения Клиента и незамедлительно уведомляет Клиента о возможности исполнения ЭСП при отсутствии иных оснований для приостановления исполнения ЭСП Клиента в соответствии с законодательством Российской Федерации или настоящими Правилами.

7. ПРАВА И ОБЯЗАННОСТИ БАНКА

7.1. Банк вправе:

7.1.1. По своему усмотрению без уведомления Клиента блокировать доступ к Системе.

7.1.2. В любое время потребовать от Клиента сменить пароль в целях защиты информации.

7.1.3. Заблокировать логин Клиента в случае отказа Клиента от использования СМС-подтверждения платежей, либо при наличии обоснованных подозрений в Компрометации.

7.1.4. Не производить исполнение полученных от Клиента ЭД и требовать от Клиента предоставления оформленных в установленном порядке платежных документов на бумажном носителе при наличии обоснованных подозрений в нарушении Клиентом действующего законодательства РФ. Банк обязан незамедлительно, но не позднее 24 (Двадцати четырех) часов, любым способом сообщить Клиенту о возникновении подобных подозрений и необходимости представить платежные документы на бумажном носителе.

7.1.5. Приостановить использование Клиентом Системы до получения от Клиента достоверной информации в случае нарушения Клиентом обязанности по предоставлению Банку достоверной информации для связи с Клиентом или обновленной информации в случае ее изменения. При этом Банк прекращает обработку всех ЭД, полученных от Клиента и не исполненных до момента блокировки.

7.1.6. Не возмещать Клиенту сумму операции, совершенной без согласия Клиента, в случаях, когда: Банк исполнил обязанность по информированию Клиента о совершенной операции и/или Клиент не направил Банку уведомление о Компрометации.

7.1.7. В одностороннем порядке приостановить до момента устранения неисправности использование Системы Клиентом в случае возникновения технических неисправностей или других обстоятельств, препятствующих использованию Клиентом Системы. Все документы в этом случае должны передаваться сторонами на бумажных носителях.

7.1.8. При непогашении Клиентом задолженности перед Банком, Банк имеет право:

- ограничить перечень услуг, предоставляемых Системой;
- приостановить оказание услуг ДБО;
- прекратить оказание услуг ДБО.

7.1.9. После предварительного уведомления Клиента приостанавливать использование Системы при несоблюдении Клиентом настоящих Правил, а также в рамках исполнения рекомендаций/требований Банка России, норм действующего законодательства РФ, в том числе, в области противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансирования терроризма. Уведомление в форме электронного сообщения по Системе направляется Банком Клиенту в срок не позднее 24 (Двадцати четырех) часов до момента приостановления использования Системы с указанием документов/информации, которые необходимо представить в Банк.

7.2. Банк обязан:

7.2.1. Производить регистрацию Участника системы в течение 3 (трех) рабочих дней с момента поступления в Банк Заявления.

7.2.2. Принимать к исполнению ЭД, полученные по Системе от Клиента, подписанные необходимым количеством ПЭП уполномоченных должностных лиц Клиента.

7.2.3. Информировать Клиента о совершенных операциях в Системе одним из способов, установленных настоящими Правилами.

7.2.4. Предоставлять Клиенту необходимые рекомендации для работы в Системе путем размещения на информационных стендах в операционных залах Банка, официальном интернет-сайте Банка в сети Интернет и/или путем направления информационных сообщений в Системе.

7.2.5. В случае получения от Клиента надлежащим образом заверенного Уведомления о прекращении действия и (или) об утрате и (или) об использовании без согласия Клиента Средства подтверждения и (или) Компрометации заблокировать логин Клиента в Системе, Средства

подтверждения и прекратить обработку ЭД, подписанных/подтвержденных указанными средствами. Исполнение данного уведомления производится Банком в срок, указанный Клиентом в уведомлении, но не ранее дня, следующего за днем получения уведомления. При наличии технической возможности, Банк может исполнить указанное уведомление в более короткий срок.

7.2.6. Возместить Клиенту сумму операций в случае совершения Банком без согласия Клиента расходных операций по расчетному счету Клиента после получения Банком от Клиента Уведомления о прекращении действия и (или) об утрате и (или) об использовании без согласия Клиента средства подтверждения и/или Компрометации.

7.2.7. Возместить Клиенту сумму операции, о которой Клиент не был проинформирован и, которая была совершена без согласия Клиента в случае неисполнения Банком обязанности по информированию Клиента о совершенной операции.

7.2.8. Фиксировать факт получения от Клиента уведомления о прекращении действия и/или об утрате и (или) об использовании без согласия Клиента Средства подтверждения и (или) Компрометации, оформленного на бумажном носителе, с обязательным указанием даты и времени получения указанного уведомления на Клиентском и своем экземплярах.

7.2.9. Хранить направленные Клиенту и полученные от клиента Уведомления о прекращении действия и(или) об утрате и (или) об использовании без согласия Клиента средства подтверждения и (или) Компрометации в течение срока не менее трех лет.

7.2.10. Рассматривать заявления/уведомления Клиента, в том числе при возникновении споров, связанных с использованием Клиентом Системы, а также предоставить Клиенту возможность получать информацию о результатах рассмотрения заявлений/уведомлений, в том числе в письменной форме по требованию Клиента, в срок не более 30 (тридцати) дней со дня получения таких заявлений/уведомлений.

7.2.11. Возмещение Клиенту суммы операции производится на указанный Клиентом счет в срок не более 30 (тридцати) дней после завершения разбора конфликтной ситуации в соответствии с действующим на момент рассмотрения конфликтной ситуации Положением о процедуре разбора конфликтных ситуаций в рамках использования дистанционного банковского обслуживания системы Faktura.ru (Приложение № 11.2 к Правилам) при условии подтверждения по результатам работы комиссии факта неисполнения Банком обязанности по информированию Клиента об оспариваемой операции.

8. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ДОКУМЕНТОВ И ИНФОРМАЦИИ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ

8.1. Клиент имеет право запрашивать у Банка документы, связанные с использованием Системы, в том числе копию Заявления о предоставлении доступа сотруднику организации в систему Faktura.ru с помощью логина/пароля, копию акта разрешительной комиссии по разбору конфликтной ситуации (если ранее между Клиентом и Банком проводилась процедура разбора конфликтной ситуации), копию экспертного заключения о подлинности ПЭП (если ранее в рамках разбора конфликтной ситуации проводилась экспертиза подлинности ПЭП), иные документы. При необходимости Клиент направляет в Банк заявление в письменном виде в свободной форме с требованием о предоставлении одного или нескольких указанных документов.

8.2. Банк в течение 5 (Пяти) рабочих дней направляет Клиенту запрашиваемые им документы по адресу, указанному в заявлении.

ЗАЯВЛЕНИЕ о предоставлении доступа сотруднику организации в Систему Faktura.ru с помощью логина/пароля

Полное наименование юридического лица/Ф.И.О. индивидуального предпринимателя/ Ф.И.О. физического лица занимающегося в установленном законодательством РФ порядке частной практикой - далее Клиент	
ИНН:	
Телефон:	
Адрес эл. почты:	

Настоящим заявлением Клиент:

Просит осуществлять дистанционное банковское обслуживание с использованием Системы Faktura.ru. При использовании Системы Faktura.ru Клиент предоставляет право подписи/наделяет полномочиями по доступу в Систему Faktura.ru, подписанию электронной подписью, подтверждению одноразовым паролем и направлению в ООО «Вайлдберриз Банк» электронных документов, в том числе с целью распоряжения денежными средствами на Счете(ах) следующих должностных лиц:

Фамилия, имя, отчество	Номер мобильного телефона	Вид ЭП
		Одноразовый пароль

Количество включаемых в печатную форму строк варьируется в зависимости от количества уполномоченных должностных лиц, которым предоставляется право подписи и распоряжения денежными средствами на Счете(-ах) Клиента.

Клиент наделяет полномочиями по доступу в Систему Faktura.ru без права подписи/распоряжения денежными средствами на Счете(-ах) следующих лиц:

Фамилия, имя, отчество	Номер мобильного телефона	Вид ЭП
		Одноразовый пароль

Количество включаемых в печатную форму строк варьируется в зависимости от количества лиц, которым предоставляется право по доступу в Систему Faktura.ru без права подписи/распоряжения денежными средствами на Счете(-ах).

Должность (при наличии)	подпись	(Ф.И.О.)
М.П.		«_____» _____ 20__ г.

Электронная подпись

ОТМЕТКИ БАНКА¹

Заявление принял:

(должность уполномоченного лица Банка)	(подпись)	(ФИО)
		«_____» _____ 20__ г.

¹ Заполняется в случае предоставления Заявления в подразделение Банка на бумажном носителе.

ПОЛОЖЕНИЕ О ПРОЦЕДУРЕ РАЗБОРА КОНФЛИКТНОЙ СИТУАЦИИ В РАМКАХ ИСПОЛЬЗОВАНИЯ СИСТЕМЫ ФАКТУРА.RU В ООО «ВАЙЛДБЕРРИЗ БАНК»

1. Настоящее положение о процедуре разбора конфликтной ситуации в рамках использования дистанционного банковского обслуживания системы Faktura.ru (далее – Положение) разработано в соответствии с Гражданским кодексом Российской Федерации, Федеральным Законом от 27.06.2011 № 161-ФЗ «О национальной платежной системе» и Федеральным Законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», является порядком досудебного урегулирования споров между Банком и Клиентом возникающих в рамках оказания услуг ДБО, в соответствии с Правилами оказания услуг дистанционного банковского обслуживания юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством РФ порядке частной практикой, в системе Faktura.ru в ООО «Вайлдберриз Банк» (далее – Правила).

2. Термины, применяемые в рамках настоящего Положения, используются в следующих значениях:

Конфликтная ситуация – спор между Клиентом и Банком (далее – Стороны) по причине перевода денежных средств, в рамках которого Клиентом оспаривается факт перевода денежных средств, подлинность электронной подписи в электронном документе и (или) факт уведомления о переводе денежных средств, возникшие в результате воздействия вредоносного кода, компрометации Средства подтверждения платежа или по иным причинам.

Разрешительная комиссия – орган, формируемый Банком в соответствии с настоящим Положением с целью разбора Конфликтной ситуации по существу и документального оформления результатов работы.

3. Подлежат рассмотрению споры, связанные с наличием у Клиента к Банку претензий по поводу:

- факта передачи Клиентом Банку электронного документа;
- дня и времени передачи Клиентом Банку электронного документа;
- содержания переданного Клиентом Банку электронного документа.

4. В случае возникновения конфликтной ситуации Сторона, обнаружившая возникновение Конфликтной ситуации, должна незамедлительно направить уведомление о Конфликтной ситуации другой Стороне. До направления уведомления иницилирующая Сторона должна убедиться, что причиной возникновения конфликта не является нарушение ей требований к защите Системы.

Уведомление о наличии Конфликтной ситуации должно содержать информацию о существовании Конфликтной ситуации и обстоятельствах, которые, по мнению уведомителя, свидетельствуют о наличии Конфликтной ситуации, а также все реквизиты соответствующего электронного документа, на основании которого Банк выполнил, не выполнил или выполнил ненадлежащим образом какую-либо операцию.

Уведомление также должно содержать фамилии, имена, отчества и должности представителей заявителя, уполномоченных вести от его имени переговоры по урегулированию Конфликтной ситуации, а также их контактные телефоны, факс, адрес электронной почты.

Уведомление о наличии Конфликтной ситуации оформляется и отправляется в виде электронного документа в Системе или в письменной форме, которое направляется нарочным либо иным способом, обеспечивающим подтверждение вручения корреспонденции адресату.

5. Сторона, которой направлено уведомление, обязана не позднее двух рабочих дней после его получения проверить наличие обстоятельств, свидетельствующих о возникновении Конфликтной ситуации, и направить уведомителю информацию о результатах проверки и, в случае необходимости, о мерах, принятых для разрешения возникшей Конфликтной ситуации.

6. Конфликтная ситуация признается разрешенной в рабочем порядке в случае, если уведомитель удовлетворен информацией, полученной от другой Стороны. В случае если уведомитель не удовлетворен информацией, полученной от другой Стороны, для рассмотрения Конфликтной ситуации формируется разрешительная комиссия.

7. Банк не позднее чем на следующий рабочий день после того, как принято решение о необходимости формирования разрешительной комиссии, но не позднее пяти рабочих дней после получения уведомления о Конфликтной ситуации, в случае если конфликтная ситуация не была урегулирована в рабочем порядке:

- формирует состав разрешительной комиссии;

- определяет дату, время и место работы разрешительной комиссии;
- информирует Клиента о назначенной дате, времени, месте работы разрешительной комиссии и о ее составе.

Если Банк и Клиент не договорятся об ином, в состав разрешительной комиссии входит равное количество уполномоченных представителей каждой из Сторон (не более трех с каждой стороны, включая владельца оспариваемой электронной подписи).

Права лиц на представление Сторон в комиссии подтверждаются доверенностями, оформленными надлежащим образом, или распорядительными актами стороны, которую они представляют.

8. Заседание разрешительной комиссии должно быть организовано Банком не позднее 10 (Десяти) рабочих дней с момента получения заявления Клиента.

9. В случае если Клиент не направит своих представителей для участия в работе разрешительной комиссии, разбор Конфликтной ситуации осуществляется без представителей Клиента.

10. Максимальный срок работы разрешительной комиссии не может превышать 20 (Двадцать) рабочих дней с даты ее формирования.

11. При работе разрешительной комиссии, каждая из сторон обязуются способствовать работе комиссии и не допускать отказа от предоставления необходимых документов (информации), если предоставление таких документов (информации) будет допустимо в соответствии с действующим законодательством РФ. Стороны обязуются предоставить разрешительной комиссии возможность ознакомления с условиями и порядком работы своих программных и аппаратных средств, используемых для обмена ЭД по Системе.

12. Сформированная разрешительная комиссия при рассмотрении Конфликтной ситуации анализирует:

- предмет разногласий на основании претензии одной из сторон;
- банковскую операцию, относящуюся к предмету разногласий;
- факт входа под логином Уполномоченного должностного лица в Систему, предшествующий отправке спорного электронного документа в Банк;
- факт отправления разового СМС-пароля на зарегистрированный номер Уполномоченного должностного лица;
- дату и время введения разового СМС-пароля для подтверждения факта формирования электронной подписи Уполномоченного должностного лица.

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

14. Подтверждением правильности исполнения Банком спорного электронного документа является одновременное выполнение следующих условий:

- отправленный разовый СМС-пароль совпадает с введенным разовым СМС-паролем и время ввода не просрочено;
- установлен факт входа под Логин Уполномоченного должностного лица (лиц) в Систему, предшествующий отправке спорного электронного документа в Банк;
- установлен факт отправления разового СМС-пароля на зарегистрированный номер Уполномоченного должностного лица (лиц);
- установлен факт ввода разового СМС-пароля для подтверждения факта формирования электронной подписи Уполномоченного должностного лица или факт отправки разового СМС-пароля в Систему.

15. Разрешительная комиссия не вправе давать правовую или какую-либо иную оценку установленных ею фактов.

16. По итогам работы комиссии составляется Акт, в котором содержится:

- дата и место составления Акта;
- даты и время начала и окончания работы разрешительной комиссии;
- состав комиссии;
- суть претензии Стороны;
- действия разрешительной комиссии;
- установленные обстоятельства;
- выводы разрешительной комиссии;
- указание на особое мнение члена (членов) разрешительной комиссии, в случае его наличия.
- подписи членов разрешительной комиссии.

Члены комиссии, не согласные с выводами, отраженными в Акте, подписывают Акт с возражениями либо излагают свое несогласие и выводы в письменном виде в отдельном документе, который прилагается к Акту.

17. Акт составляется в двух экземплярах - по одному для каждой из Сторон не позднее 10 рабочих дней с момента окончания работы комиссии. По требованию члена разрешительной комиссии ему может быть выдана заверенная Банком копия Акта. Один из экземпляров Акта направляется Банком Клиенту по Системе, нарочным, либо иным способом, обеспечивающим подтверждение вручения корреспонденции адресату.
18. Выводы, содержащиеся в Акте, являются обязательными для Сторон. В случае если подписание Акта в установленный срок не состоится, заинтересованная Сторона вправе обратиться в Арбитражный суд и без выработанного Сторонами решения.
19. Результатом рассмотрения спорной ситуации разрешительной комиссией является определение Стороны, несущей ответственность согласно выводу о подлинности электронной подписи Клиента под электронным документом.
20. В случае подтверждения правильности исполнения Банком спорного электронного документа Клиента претензии Клиента к Банку, связанные с последствиями исполнения указанного электронного документа Клиента, признаются необоснованными.
21. В случае, если будет установлено, что правильность исполнения электронного документа Клиента не подтверждена, т.е. проверяемый электронный документ Клиента подтвержден некорректной электронной подписью, либо электронный документ Клиента не был правильно исполнен Банком. В этом случае претензии Клиента к Банку, связанные с последствиями исполнения указанного электронного документа Клиента, признаются обоснованными.
22. В случае принятия Банком решения о возмещении Банком Клиенту суммы операции, совершенной с использованием Системы и без согласия Клиента, сумма возмещения зачисляется на счет Клиента в течение 7 (семи) календарных дней с момента принятия решения.

**ЗАЯВЛЕНИЕ
на настройку лимитов в Системе Faktura.ru**

Полное наименование юридического лица/Ф.И.О. индивидуального предпринимателя/ Ф.И.О. физического лица занимающегося в установленном законодательством РФ порядке частной практикой - далее Клиент	
ИНН:	
Адрес места нахождения:	
Телефон:	

Настоящим заявлением Клиент просит включить суточный лимит платежей на сумму платежей в течение одного дня (календарные сутки по московскому времени) в размере:

_____ (сумма цифрами) _____ (сумма прописью)

_____ Должность (при наличии) _____ подпись _____ (Ф.И.О.)

М.П.

« _____ » _____ 20__ г.

Электронная подпись

ОТМЕТКИ БАНКА²

Заявление принял:

_____ (должность уполномоченного лица Банка) _____ (подпись) _____ (ФИО)

« _____ » _____ 20__ г.

² Заполняется в случае предоставления Заявления в подразделение Банка на бумажном носителе.

УВЕДОМЛЕНИЕ
о прекращении действия и (или) об утрате/компрометации
средства подтверждения и(или) использовании средства подтверждения без согласия
Клиента и(или) о приостановлении/прекращении использования Системы Faktura.ru в ООО
«Вайлдберриз Банк»

Полное наименование юридического лица/Ф.И.О. индивидуального предпринимателя/ Ф.И.О. физического лица занимающегося в установленном законодательством РФ порядке частной практикой - далее Клиент	
ИНН:	
Адрес места нахождения:	

Настоящим Клиент:

1. Уведомляет Банк:

☐ о прекращении действия средства подтверждения
☐ об утрате/компрометации средства подтверждения
☐ об использовании средства подтверждения без согласия Клиента

Прошу с «__» _____ 20__ г. заблокировать указанное ниже средство подтверждения, использовавшееся в соответствии с Правилами оказания услуг дистанционного банковского обслуживания юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством РФ порядке частной практикой, в Системе Faktura.ru в ООО «Вайлдберриз Банк», и остановить обработку электронных документов, подписанных/подтвержденных указанным средством:

☐ мобильный телефон

Фамилия, имя, отчество уполномоченного должностного лица	Номер телефона	Адрес электронной почты

2. Уведомляет Банк:

☐ о приостановлении использования Системы Faktura.ru ☐ о прекращении использования Системы Faktura.ru

Прошу с 00:00 «__» _____ 20__ г. заблокировать все средства подтверждения и прекратить обработку электронных документов, подписанных/подтвержденных средствами подтверждения.

_____	_____	_____
Должность (при наличии)	подпись	(Ф.И.О.)

М.П. _____ «__» _____ 20__ г.

Электронная подпись

ОТМЕТКИ БАНКА

Заявление принял:

_____	_____	_____
(должность уполномоченного лица Банка)	(подпись)	(ФИО)

ОРГАНИЗАЦИОННЫЕ МЕРЫ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОЙ РАБОТЫ В СИСТЕМЕ FAKTURA.RU

1. Требования по защите от вредоносного кода:

1.1. К средствам защиты от вредоносного кода относятся средства, используемые для:

- выявления и обезвреживания вредоносного кода (антивирусы);
- межсетевого экранирования рабочего места или корпоративной сети;
- Web-фильтрации;
- обнаружения и предотвращения вторжений;
- контроля выполнения приложений.

2. Для обеспечения надлежащей защиты от вредоносного кода Клиент обязан:

- обеспечить непрерывное использование средств защиты от вредоносного кода;
- обеспечить периодический контроль целостности системного, прикладного и специального программного обеспечения;
- ежедневно осуществлять проверку рабочего места на наличие вредоносного кода;
- обеспечить регулярное обновление средств защиты от вредоносного кода, обновление прикладного программного обеспечения, установку пакетов обновления безопасности операционной системы;
- использовать лицензионное программное обеспечение;
- использовать для работы в Системе учетную запись, не входящую в группу «Локальные администраторы» или аналогичную группу пользователей;
- на мобильном устройстве (смартфоне) не повышать полномочия до пользователя root;
- осуществлять вход в Систему с рабочего места используемого исключительно для подключения к Системе;
- ограничивать по времени доступ ответственных лиц к ПЭП и/или телефону, на который приходят СМС – подтверждения платежей;
- контролировать суммы переводов, реквизиты получателей.

3. Для защиты ПЭП необходимо:

3.1. Для входа в Систему вводить логин и пароль только на сайте Системы, убедиться в подлинности сайта Системы до ввода реквизитов доступа.

3.2. Никогда и ни при каких обстоятельствах не сообщать никому свои логины, пароли, СМС/Push коды.

3.3. Обязательно сверять текст СМС-сообщений, содержащий пароль, с деталями выполняемой операции. Если в СМС указан пароль для платежа, который вы не совершали или его предлагают ввести/назвать, чтобы отменить якобы ошибочно проведенный по счету платеж, ни в коем случае не вводить его и не сообщать его никому, в том числе сотрудникам Банка.

3.4. В случае утери мобильного телефона, на который приходят разовые пароли, немедленно заблокировать соответствующую SIM-карту у оператора сотовой связи.

3.5. Записать контактный телефон Банка в адресную книгу или запомнить его. В случае если в личном кабинете Системы вы обнаружите телефон, отличный от записанного, в особенности, если вас будут призывать позвонить по этому телефону для уточнения информации, либо по другому поводу, будьте бдительны и немедленно позвоните в Банк по ранее записанному вами телефону.

3.6. Устанавливать мобильные приложения Системы только из авторизованных магазинов. Использовать антивирусное программное обеспечение для смартфона.

3.7. Избегать регистрации номера мобильного телефона, на который приходят СМС-сообщения с разовым паролем, в социальных сетях и других открытых источниках.

4. Общие правила безопасности, применяющиеся для защиты любых данных, хранящихся на компьютерах:

4.1. Использовать только компьютеры с лицензионным программным обеспечением, установленным и запущенным антивирусным программным обеспечением и персональным межсетевым экраном, своевременно обновлять антивирусные базы. Регулярно проводить полную проверку компьютера на предмет наличия вредоносного кода, своевременно обновлять лицензионную операционную систему и браузеры.

- 4.2. Проверять действительность сертификата веб-сайта Системы. При вводе личной информации, помнить, что любой веб-адрес в адресной строке Интернет-банка должен начинаться с «https». Если в адресе не указано «https», это значит, что вы находитесь на незащищенном веб-сайте, и вводить данные нельзя.
- 4.3. Использовать виртуальную клавиатуру для ввода пароля.
- 4.4. Быть внимательным: в случае возникновения подозрений на мошенничество необходимо максимально быстро сообщить о своих подозрениях в Банк с целью оперативного блокирования доступа к вашей учетной записи в Системе.
- 4.5. При работе с электронной почтой не открывать письма и вложения к ним, полученные от неизвестных отправителей, не переходить по содержащимся в таких письмах ссылкам.
- 4.6. Не работать с правами администратора при отсутствии необходимости. В повседневной практике входить в систему как пользователь, не имеющий прав администратора.
- 4.7. Включить системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически просматривать журнал и реагировать на ошибки.
- 4.8. Запретить в межсетевом экране соединения по неиспользуемым протоколам.
- 4.9. Не давать разрешения неизвестным программам выходить в Интернет.
- 4.10. При работе в Интернете не соглашаться на установку каких-либо дополнительных программ от недоверенных издателей.