Приложение № 11
к Договору на обслуживание Клиента
в системе дистанционного банковского
обслуживания «iBank2»

Порядок действий Сторон в случае выявления хищения денежных средств в системе «iBank2»

1. Клиенту в случае выявления хищения денежных средств в системе «iBank2» необходимо:

1.1. Немедленно прекратить любые действия с ЭУ, подключенным к системе «iBank2», обесточить его (принудительно отключить электропитание в обход штатной процедуры завершения работы, извлечь все аккумуляторные батареи из ноутбука и т.п.) и отключить от информационных сетей (если было подключение, например, по Ethernet, USB, Wi-Fi, Dial-Up и др.) или перевести в режим гибернации («спящий» режим).

При отсутствии возможности обесточивания ЭУ, осуществить отключение по штатной процедуре и запротоколировать указанный факт.

1.2. При наличии технической возможности отозвать распоряжение на перевод денежных средств с использованием иного ЭУ, после чего принять меры к блокировке системы «iBank2».

1.3. При отсутствии технической возможности отозвать распоряжение на перевод денежных средств по системе «iBank2» немедленно обратиться в Банк по контактным телефонам, указанным в Заявлении (Оферте) о присоединении к Договору на обслуживание Клиента в системе дистанционного банковского обслуживания «iBank2», с заявлением о блокировке системы «iBank2», приостановке исполнения распоряжения на перевод денежных средств и возврате денежных средств.

1.4. Произвести фотосъемку ЭУ (с подключенными кабелями и иными периферийными устройствами), рабочего места и его расположения в помещении. Обеспечить сохранность (целостность) ЭУ как возможного средства совершения преступления, поместив его в место с ограниченным доступом, обеспечив при этом защиту от вскрытия (стикеры, наклейки, пластилин, мастичная печать, пломбы и т.п.) и по возможности зафиксировать средства контроля целостности фотографированием со всех ракурсов. Если позволяют размеры ЭУ, следует поместить его в непрозрачный пакет (мешок) и заклеить горловину. При необходимости ведения хозяйственной деятельности - задействовать другое ЭУ.

1.5. Дополнительно к действиям, перечисленным в пп. 1.2., 1.3. настоящего Порядка, обратиться в Банк с письменным заявлением об отзыве распоряжения на перевод денежных средств, возврате денежных средств и блокировании доступа к системе «iBank2» (Приложение № 11.1. к настоящему Договору), а также о компрометации ключей ЭП и необходимости смены ключей ЭП. Копия заявления должна быть направлена в Банк незамедлительно по факсу или по электронной почте (скан-копия). Оригинал заявления должен быть доставлен в Банк течение одного дня.

1.6. Проинформировать все кредитные организации, с которыми Клиент имеет договорные отношения, предусматривающие использование систем ДБО, о факте хищения денежных средств и обратиться с просьбой о внеплановой замене ключевой информации.

1.7. При наличии необходимой информации обратиться в банк-получателя или к оператору соответствующей платежной системы с письменным заявлением о приостановлении зачисления денежных средств на счет получателя и возврате денежных средств (Приложение № 11.2. к настоящему Договору).

1.8. Предпринять меры для обеспечения сохранности и неизменности записей с внутренних и внешних камер систем видеонаблюдения, журналов систем контроля доступа, средств обеспечения и разграничения доступа в сеть Интернет (при наличии таковых) за максимальный период времени, как до, так и после даты совершения хищения денежных средств.

1.9. Провести сбор записей с межсетевых экранов и других средств защиты информации, серверов баз данных и иных компонент клиентского приложения системы «iBank2», систем авторизации пользователей (AD, NDS и т.д.), коммуникационного оборудования (включая АТС), ЭУ, устройств, которые могут использоваться для удаленного управления указанными ЭУ.

1.10. При возможности оперативно обратиться с письменным заявлением к своему Интернет-провайдеру или оператору связи (Приложение № 11.3. к настоящему Договору) для получения в электронной форме журналов соединений с сетью Интернет с ЭУ клиента или из его локальной вычислительной сети (далее - ЛВС) как минимум за три месяца, предшествовавшие факту хищения денежных средств.

1.11. Не предпринимать никаких действий для самостоятельного или с привлечением сторонних ИТ-специалистов поиска и удаления компьютерных вирусов, восстановления работоспособности ЭУ, не отправлять ЭУ в сервисные службы для восстановления работоспособности.

1.12. Зафиксировать в протокольной форме значимые действия и события, в том числе имена лиц, имеющих доступ к ЭУ, действия с ЭУ, подключенным к системе «iBank2», предшествовавшие факту хищения денежных средств, подготовить объяснения работников Клиента об использовании ЭУ в целях, отличных от осуществления операций в системе «iBank2», посещаемых интернет-сайтах, о странностях при работе ЭУ, перебоях или отказах ЭУ, обращениях в ИТ-службы, в Банк, о сторонних лицах, побывавших в месте расположения ЭУ и т.д.

1.13. Все действия, указанные в пп. 1.1., 1.4., 1.8., 1.9., 1.12. настоящего Порядка, производить коллегиально, протоколировать и документировать, в т.ч. с использованием фотосъемки.

При невозможности осуществления коллегиальных действий отдельно зафиксировать данный факт.

1.14. Оперативно обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств (Приложение № 11.4. к настоящему Договору).

1.15. Оперативно обратиться в суд с исковым заявлением в отношении получателя денежных средств (указав все известные реквизиты получателя) о взыскании неосновательно полученного обогащения и процентов за пользование денежными средствами (глава 60 ГК РФ), а также с ходатайством о принятии судом мер по обеспечению иска в виде ареста денежных средств на счете получателя в сумме неосновательно полученного обогащения. К исковому заявлению необходимо приложить копию заявления о возбуждении уголовного дела либо копию талона, содержащего порядковый номер из книги учета сообщений о преступлениях (далее - КУСП) содержащую отметку правоохранительного органа о его приеме.

1.16. Копии вышеуказанных документов направить в Банк с приложением Справки по факту инцидента информационной безопасности в системе «iBank2» (Приложение № 11.5. к настоящему Договору), а также подтверждающих документов (Приложение № 11.6. к настоящему Договору).

2. Сотрудники Банка в случае выявления хищения денежных средств в системе «iBank2»:

2.1. При получении телефонного обращения Клиента-плательщика о приостановке исполнения распоряжения о переводе денежных средств немедленно предпринимают разумно возможные и достаточные действия для идентификации Клиента-плательщика, в том числе, посредством использования контактной информации, указанной в договоре банковского счета. При наличии возможности используют дополнительные каналы для подтверждения обращения (SMS-уведомление, сообщение по электронной почте).

2.2. При подтверждении обращения Клиента незамедлительно принимают меры к приостановке дальнейшей обработки платежа. При невозможности аутентификации Клиента-плательщика, фиксируют данный факт, и продолжают обработку платежа, если нет иных оснований для приостановки дальнейшей обработки платежа.

2.3. В случае завершения обработки платежа незамедлительно в любой доступной форме направляют в службу безопасности банка-получателя информацию о факте хищения денежных средств с просьбой о приостановке обработки платежа.

2.4. Оперативно направляют с использованием сервисов расчетной системы Банка России в банк-получателя сообщение с просьбой о приостановлении платежа и возврате денежных средств.

2.5. С целью обеспечения сохранности доказательств исключают доставку в Банк и/или техническое обслуживание ЭУ Клиента, консультации, проверки ЭУ Клиента, а равно совершение сотрудниками Банка иных действий, которые могут привести к нарушению сохранности доказательств.

2.6. Оперативно направляют письмо в банк-получателя или оператору платежной системы по факту хищения денежных средств с просьбой о прекращении обработки платежа, блокировке системы ДБО и платежных карт клиента - получателя, применении к получателю платежа мер контроля в рамках системы ПОД/ФТ, предусмотренных Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», и возврате денежных средств.

Истребуют у Клиента-плательщика подтверждение о подаче Клиентом-плательщиком заявления в правоохранительные органы для получения его копии в течение не более 2 рабочих дней со дня получения обращения Клиента-плательщика в Банк о факте хищения денежных средств.

2.7. Подготавливают документы, указанные в Приложении № 11.7. к настоящему Договору.

2.8. Осуществляют следующие действия с привлечением сотрудников отдела информационной безопасности:

2.8.1. Проводят мероприятия, определенные настоящим Договором, в отношении проверки подлинности ЭП под оспоренным расчетным документом. При необходимости - проводят мероприятия по факту компрометации ключей ЭП.

2.8.2. Получают от сотрудников Банка, ответственных за обслуживание системы «iBank2», администраторов сети, систем криптографической защиты и т.д. экспертные заключения в рамках их компетенции по корректности ЭП в составе расчетного документа, ее целостности и авторства.

2.8.3. Проводят анализ собранной информации с целью выявления источника осуществления хищения денежных средств и возможной причастности сотрудников Банка. Документально оформляют результаты проверки.

2.8.4. При необходимости - проводят технические мероприятия, направленные на предотвращение сокрытия следов, уничтожения информации и т.д., для чего задействуют используемые в Банке средства и методы защиты информации.

2.8.5. Обеспечивают хранение собранной информации в неизменном виде для передачи правоохранительным органам по запросу.

2.9. При необходимости проводят, документально зафиксировав полученные результаты, следующие проверочные мероприятия в целях формирования необходимой доказательной базы по факту хищения

денежных средств:

2.9.1. Находят оспоренный Клиентом-плательщиком расчетный документ в базе данных системы «iBank2» и в базе данных автоматизированной банковской системы (далее - АБС) Банка.

2.9.2. Если расчетный документ не найден в базе данных «iBank2», но имеется в базе данных АБС Банка:

2.9.2.1. По журналам систем «iBank2» и АБС устанавливают, присутствовал ли расчетный документ в системе «iBank2» ранее.

2.9.2.2. В свойствах расчетного документа устанавливают его авторство, дату, время и способ его создания.

2.9.2.3. Получают объяснения от сотрудников Банка, уполномоченных на оформление и проверку расчетных документов, администраторов «iBank2» и АБС Банка, администраторов информационной безопасности «iBank2» и АБС Банка.

2.9.2.4. Проводят сбор записей с межсетевых экранов, систем обнаружения вторжений и антивирусной защиты, серверов баз данных, систем авторизации пользователей (AD, NDS и т.д.), рабочих станций сотрудников Банка, штатно допущенных к управлению системой «iBank2», и средств удаленного управления указанными рабочими станциями.

2.9.2.5. Получают записи систем видеонаблюдения, управления доступом в помещения Банка и т.д.

2.9.2.6. Оценивают возможность продолжения эксплуатации системы «iBank2».

2.9.3. Если расчетный документ найден в базе данных системы «iBank2», проверяют подлинность оспариваемого расчетного документа.

2.9.3.1. Если подлинность расчетного документа не установлена:

2.9.3.1.1. Получают объяснения от сотрудников Банка, уполномоченных на оформление и проверку расчетных документов, поступивших по системе «iBank2», администраторов системы «iBank2» и АБС Банка, администраторов информационной безопасности системы «iBank2» и АБС Банка.

2.9.3.1.2. По журналам системы «iBank2» устанавливают, была ли подлинность расчетного документа утрачена в процессе эксплуатации системы «iBank2», а также оценивают возможность продолжения эксплуатации системы «iBank2».

2.9.3.2. Если подлинность расчетного документа установлена:

2.9.3.2.1. Реализовывают неотложные действия при компрометации ключа ЭП Клиента-плательщика непосредственно после обращения Клиента.

2.9.3.2.2. Получают от уполномоченного сотрудника Банка журналы работы системы «iBank2» и анализируют их на предмет наличия записей, содержащих признаки несанкционированного доступа посторонних лиц.

2.9.3.2.3. Проводят мероприятия, направленные на обеспечение целостности носителя.

2.9.4. Проводят анализ информации с целью выявления возможной причастности к хищению денежных средств сотрудников Банка. При необходимости проводят технические мероприятия, направленные на предотвращение сокрытия следов хищения.

2.10. Получают от Клиента-плательщика Справку по факту инцидента информационной безопасности в системе «iBank2» (Приложение № 11.5. к настоящему Договору).

2.11. На основании собранной информации оформляют и передают в правоохранительный орган, осуществляющий расследование по факту хищения денежных средств, объяснение по факту хищения денежных средств. В случае отказа Клиента-плательщика от обращения в правоохранительные органы оформляют обращение по факту хищения денежных средств в региональное подразделение МВД от имени Банка.

2.12. Обращаются в Бюро специальных технических мероприятий Главного Управления МВД России с заявлением об оказании содействия в расследовании факта хищения денежных средств с подробным описанием обстоятельств его совершения, по запросу БСТМ МВД России направляют документы, указанные в Приложении № 11.7. к настоящему Договору.

2.13. В случае хищения денежных средств Клиента-плательщика, по счетам которого зафиксированы поступления средств бюджета любого уровня, также направляют информационное письмо на имя руководителя ФСБ России о факте хищения денежных средств с подробным описанием обстоятельств его совершения.

2.14. Направляют в банк-получателя полученную от Клиента-плательщика копию заявления в правоохранительный орган по факту хищения денежных средств и номер КУСП (в случае обращения в правоохранительные органы).

2.15. При наличии в Банке электронного расчетного документа Клиента с подлинной электронной подписью и при оспаривании подлинности электронной подписи в составе электронного расчетного документа, подтверждающего поручение Клиента-плательщика Банку выполнить оспоренный перевод, направляют Клиенту-плательщику письмо о готовности участия в работе экспертной комиссии с целью проверки подлинности электронной подписи.

Приложение № 11.1.
к Договору на обслуживание Клиента
в системе дистанционного банковского
обслуживания iBank2

_____
_____

ЗАЯВЛЕНИЕ

Настоящим сообщаем, что «____» _____ 201__ года с банковского счета № _____, открытого в _____, по системе дистанционного банковского обслуживания «iBank 2» были похищены денежные средства, которые, по имеющейся информации были переведены по следующими платежным реквизитам:

Дата платежа	«____» _____ 201__ г.
Номер распоряжения	
Наименование банка плательщика	
Наименование плательщика	
ИНН плательщика	
Номер счета плательщика	
Наименование банка получателя	
Наименование получателя	
ИНН получателя	
Номер счета получателя	
Сумма платежа	
Назначение платежа	

Прошу Вас заблокировать ключи электронной подписи со следующими идентификационными номерами _____ в системе дистанционного банковского обслуживания «iBank 2» и оказать содействие в возврате денежных средств.

_____ _____ (_____)
должность подпись расшифровка подписи

«___» _____ 20___ года

Исп. _____
Ф.И.О.
тел. _____

Приложение № 11.2.
к Договору на обслуживание Клиента
в системе дистанционного банковского
обслуживания iBank2

_____
должность руководителя

_____
наименование банка-получателя

_____
Ф.И.О. руководителя

ЗАЯВЛЕНИЕ

Настоящим сообщаем, что «____» _____ 201__ года с нашего банковского счета № _____, открытого в _____ (БИК _____) были похищены денежные средства, которые, по информации, полученной из ООО «ЮРБ», были переведены со следующим реквизитам платежа:

Дата платежа	«____» _____ 201__ г.
Номер распоряжения	
Наименование банка плательщика	
Наименование плательщика	
ИНН плательщика	
Номер счета плательщика	
Наименование банка получателя	
Наименование получателя	
ИНН получателя	
Номер счета получателя	
Сумма платежа	
Назначение платежа	

Прошу Вас оказать содействие в приостановлении прохождения платежа и возврате денежных средств.

_____ _____ (_____)
должность подпись расшифровка подписи

«___» _____ 20___ года

Исп. _____
Ф.И.О.
тел. _____

Приложение № 11.3.
к Договору на обслуживание Клиента
в системе дистанционного банковского
обслуживания iBank2

_____
должность руководителя
_____
наименование организации-провайдера
_____
Ф.И.О. руководителя

«___» _____ 20____ года между _____ и вами был заключен договор N _____ об оказании _____ услуг.

Настоящим сообщаю, что «___» _____ 20__ года в __:__ по московскому времени с расчетного счета _____ (далее – Счет), по системе дистанционного банковского обслуживания (далее – система ДБО) был осуществлен несанкционированный перевод денежных средств.

Компьютер, с которого осуществляется подключение к системе дистанционного банковского обслуживания (далее – ДБО), располагается по адресу: _____ и использует IP-адрес ___.___.___.___ (далее – Компьютер).

Вероятной причиной несанкционированного перевода денежных средств со Счета могло послужить заражение Компьютера вредоносным программным обеспечением, кража логина, пароля и ключей электронной подписи системы ДБО.

Для выявления обстоятельств несанкционированного перевода денежных средств со Счета прошу предоставить информацию из журналов (логов) о входящем и исходящем трафике за период с «___» _____ 20___ года по «____» _____ 20___ года с указанием времени соединения, IP и MAC адресов.

_____ _____ (_____)
должность подпись расшифровка подписи

«___» _____ 20__ года

Исп. _____
Ф.И.О.
тел. _____

Приложение № 11.4.
к Договору на обслуживание Клиента
в системе дистанционного банковского
обслуживания iBank2

Начальнику ОВД по _____
наименование ОВД
от _____
должность, ФИО заявителя
_____
наименование организации

ЗАЯВЛЕНИЕ

Прошу провести проверку настоящего заявления по факту незаконного завладения принадлежащими _____
наименование организации/ФИО потерпевшего
денежными средствами (кражи) с использованием системы дистанционного банковского обслуживания (далее - ДБО) ООО «ЮРБ».

«____» _____ 201__ г. неизвестными лицами по системе ДБО был осуществлен несанкционированный перевод денежных средств со следующими реквизитами:

Дата платежа	«____» _____ 201__ г.
Номер распоряжения	
Наименование банка плательщика	
Наименование плательщика	
ИНН плательщика	
Номер счета плательщика	
Наименование банка получателя	
Наименование получателя	
ИНН получателя	
Номер счета получателя	
Сумма платежа	
Назначение платежа	

Оснований для данного денежного перевода нет: с получателем платежа отсутствуют договорные и иные деловые отношения, равно как и какие-либо обязательства перед ним; перевод расцениваю как хищение денежных средств.

Признаком хищения является то, что этот перевод не был осуществлен уполномоченными лицами.

Факт осуществления этого перевода был установлен «___» _____ 201__ г. _____
ФИО лица, установившего факт несанкционированного перевода,
должность, наименование организации
при _____
обстоятельства обнаружения факта несанкционированного перевода

Компьютер, с которого осуществляется подключение к системе ДБО, располагается по адресу: _____, доступ к электронному устройству ограничен, прямая кража учетной записи, пароля и ключей электронной подписи маловероятна.

Вероятной причиной этого несанкционированного перевода денежных средств считаю ввод, удаление, блокирование, модификацию компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, поскольку данному событию сопутствовали следующие обстоятельства:

1. _____;
обстоятельства, снижающие вероятность прямого хищения реквизитов доступа в систему ДБО
2. _____;
наблюдавшиеся сбои, нехарактерное поведение системы ДБО и рабочего места системы ДБО
3. _____.
иное

На основании изложенного, прошу Вас провести необходимые оперативно-розыскные мероприятия для выявления виновных лиц и привлечь их к уголовной ответственности в соответствии с действующим законодательством.

_____ _____ (_____)
должность подпись расшифровка подписи
«___» _____ 20__ года

Исп. _____, тел. _____

Приложение № 11.5.
к Договору на обслуживание Клиента
в системе дистанционного банковского
обслуживания iBank2

Справка по факту инцидента информационной безопасности в системе «iBank2»

Настоящим сообщаю, что «___» _____ 20___ года неустановленным лицом через систему «iBank 2» была совершена несанкционированная операция по переводу денежных средств со следующими реквизитами:

Дата платежа	«____» _____ 201__ г.
Номер распоряжения	
Наименование банка плательщика	
Наименование плательщика	
ИНН плательщика	
Номер счета плательщика	
Наименование банка получателя	
Наименование получателя	
ИНН получателя	
Номер счета получателя	
Сумма платежа	
Назначение платежа	

Дополнительно сообщаю:

1. Количество ЭУ, используемых для доступа в систему «iBank 2»: _____.

2. Для доступа в систему «iBank 2» хотя бы раз использовались:

☐ корпоративные ЭУ

☐ личные ЭУ

☐ ЭУ, находящиеся в общественном пользовании.

3. Периодичность смены пароля для входа в систему «iBank 2»: _____.

4. Применяемые элементы безопасности ЭУ включают:

☐ используется только программное обеспечение для работы в системе «iBank 2»

☐ используется только лицензионное программное обеспечение

☐ операционная система и приложения обновляются в автоматическом режиме

☐ используется антивирусное программное обеспечение: _____

☐ антивирусное программное обеспечение обновляется ежедневно

☐ из числа съемных носителей информации на ЭУ используются только носители ключевой информации

☐ передача файлов и обмен сообщениями по электронной почте на ЭУ ограничены

☐ используются средства сетевой защиты: _____

☐ на ЭУ запрещены входящие соединения из сети Интернет

☐ запрещено удаленное управление ЭУ

☐ с ЭУ разрешены исходящие соединения с Банком и ограниченным числом сайтов сети Интернет для проведения обновлений программного обеспечения, число разрешенных сайтов составляет _____

☐ обеспечивается возможность доступа к ЭУ только уполномоченных лиц

☐ обеспечивается возможность доступа к носителям ключевой информации только уполномоченных лиц

☐ часы работы Клиента

☐ список лиц, имеющих доступ к НКИ

☐ список лиц, имеющих доступ к ЭУ

Иная информация, имеющая отношение к инциденту: _____

_____ _____ (_____)
должность подпись расшифровка подписи

☐ _____ **намерено** обратиться в правоохранительные органы по факту
(название Клиента)
хищения денежных средств

Заявление в правоохранительные органы принято в ОВД _____
район, округ, город, субъект федерации и иные идентифицирующие ОВД данные и зарегистрировано за N _____ в КУСП

☐ _____ **не намерено** обратиться в правоохранительные органы по факту
(название Клиента)
хищения денежных средств

О необходимости предоставления доступа сотрудников правоохранительных органов к электронному устройству предупрежден.

_____ _____ (_____)
должность подпись расшифровка подписи

«___» _____ 20__ года

Исп. _____, тел. _____

Приложение № 11.6.
к Договору на обслуживание Клиента
в системе дистанционного банковского
обслуживания iBank2

Перечень документов, которые могут быть истребованы у клиента-плательщика в случае выявления хищения денежных средств

1. Копия лицензии на операционную систему электронного устройства (далее – ЭУ).

2. Описание используемого ПО (перечень использованного лицензионного ПО на рабочем месте, информация о версии операционной системы и наличии критических обновлений, рекомендуемых разработчиком операционной системы).

3. Копия договора на оказание телематических услуг информационно-телекоммуникационной сети Интернет.

4. Описание организации доступа в сеть Интернет на рабочем месте.

5. Копия заявления в правоохранительные органы.

6. Копия лицензии на антивирусное ПО.

7. Копия документа, подтверждающего легальность антивирусного ПО.

8. Описание средств антивирусной защиты рабочего места (наличие установленного на жестком диске ЭУ Клиента антивирусного программного обеспечения и актуальность его баз, частота обновления, сканирования, наличие сведений о проявлении на ЭУ Клиента вредоносных программ и пр.).

9. Описание системы защиты информации (наличие или отсутствие персонального межсетевого экрана у Клиента, сведения об использовании рабочего места в иных целях, кроме осуществления операций в системе «iBank2», в частности - интернет-серфинга, сведения о порядке хранения и использования носителей ключевой информации).

Приложение № 11.7.
к Договору на обслуживание Клиента
в системе дистанционного банковского
обслуживания iBank2

Перечень документов в отношении потерпевшего Клиента, на счет которого неправомерно зачислены денежные средства

1. Договор банковского счета, договор на обслуживание Клиента в системе дистанционного банковского обслуживания «iBank2».

2. Сведения о точном месте открытия и месте нахождения счета Клиента.

3. Заверенная копия карточки с образцами подписей и оттиска печати Клиента.

4. Расширенная выписка по Счету Клиента с отражением сведений о движении денежных средств в период осуществления несанкционированного перевода.

5. Заверенные копии платежных документов, на основании которых были несанкционированно переведены денежные средства.

6. Носитель информации, содержащий записи видеокамер, имеющие отношение к хищению (до процессуального изъятия оригинала технического носителя информации следует обеспечить сохранность записей).

7. Документы, отражающие статистику соединений с системой «iBank2», с указанием учетных записей, внешних IP-адресов Клиента и точного времени соединений в период осуществления несанкционированного перевода.

8. Сведения о представителях Клиента, имеющих право первой и второй подписи, в том числе электронной подписи расчетных документов.

9. Сведения о подключенных уведомительных услугах Банка (СМС-уведомление, голосовая авторизация, уведомление на электронную почту, привязка к выделенному IP-адресу и другие имеющиеся услуги) с приложением копий документов, акцептованных Банком при предоставлении указанных услуг.

10. Материалы, подготовленные Банком по итогам проведения внутренних проверок.