Регламент взаимодействия Клиента и Банка в случае выявления хищения или подозрения на хищение денежных средств Клиента в системе «ТКВ Express»

1. Общие положения

1.1. Настоящий Регламент является неотъемлемой частью Договора на обслуживание Клиента – физического лица (далее – Клиента) с использованием системы «ТКВ Express» (далее - Договор).

1.2. Регламент взаимодействия Клиента и Банка в случае выявления хищения или возникновения подозрения на хищение денежных средств Клиента в системе «ТКВ Express» (далее – Регламент) определяет последовательность действий Клиента и сотрудников Банка при выявлении хищения (подозрении на хищение) денежных средств Клиента с использованием системы дистанционного банковского обслуживания «ТКВ Express» (далее - Система).

1.3. Под хищением в соответствии со ст. 158 Уголовного кодекса РФ, понимаются совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившие ущерб собственнику или иному владельцу этого имущества.

1.4. В рамках настоящего Регламента Стороны договорились считать хищением любую завершенную несанкционированную Клиентом операцию с денежными средствами на его Счетах, выполненную в Системе, и направленную на изъятие денежных средств Клиента, при условии, что данная операция не является обязанностью Банка по выполнению законодательства РФ.

1.5. В рамках настоящего Регламента Стороны договорились считать подозрением на хищение денежных средств любую незавершенную несанкционированную Клиентом операцию с денежными средствами на его Счетах, выполненную в Системе, и направленную на изъятие денежных средств Клиента, при условии, что данная операция не является обязанностью Банка по выполнению законодательства РФ.

1.6. Подписывая Договор, Клиент дает свое согласие и подтверждает намерение совершения необходимых действий для соблюдения настоящего Регламента в случае выявления хищения или подозрения на хищение денежных средств, находящихся на его Счетах, с использованием Системы.

1.7. Стороны Договора признают, что последовательность действий как Клиента, так и сотрудников Банка, описанная в настоящем Регламенте, является достаточной мерой, направленной на возврат денежных средств Клиента или предотвращение хищения денежных средств Клиента.

1.8. Любые действия Клиента и сотрудников Банка, направленные на возврат денежных средств Клиента или на предотвращение хищения денежных средств с его Счетов, не должны выходить за рамки действующего законодательства Российской Федерации.

1.9. Клиент осведомлен и согласен, что в случае хищения денежных средств он не должен настаивать на осмотре, проверке работоспособности и иных действиях с электронными устройствами (далее – ЭУ), которые использовались им для доступа в Систему, сотрудниками Банка. Банк не несет никакой материальной, административной и иной ответственности за сохранность доказательств, подтверждающих факт хищения или попытки хищения денежных средств, сохранность иной информации, хранящейся на электронном устройстве и дальнейшую работоспособность ЭУ.

2. Последовательность действий Клиента при выявлении хищения или попытки хищения денежных средств.

2.1. При выявлении хищения денежных средств или подозрении на хищение денежных средств:

2.1.1. Клиент немедленно прекращает любые действия с ЭУ, используемым для работы в Системе, обесточивает его (принудительно отключает электропитание в обход штатной процедуры завершения работы, извлекает все аккумуляторные батареи из ноутбука, телефона и т.п.) и отключает от информационных сетей (если было подключение, например, по USB, Wi-Fi и др.) или переводит в режим гибернации (сна). При отсутствии возможности обесточивания ЭУ, осуществляет отключение по штатной процедуре.

2.1.2. Клиент отзывает электронный документ (далее – ЭД), содержащий поручение на несанкционированную (завершенную или незавершенную) операцию с денежными средствами, обратившись в Банк, следующими способами: при наличии технической возможности отзыва ЭД - с использованием иного ЭУ, после чего блокирует доступ в Систему, обратившись в Банк по телефону Службы «Контакт-центр» (+7 (495) 777 4150 или для звонков из регионов России +7 (800) 100 3200) и назвав Блокировочное слово.

2.1.3. При отсутствии технической возможности отзыва ЭД в Системе, Клиент немедленно обращается в Банк по телефону с заявлением о приостановке обработки ЭД и возврате денежных средств.

2.1.4. Не позднее дня, следующего за днем обращения Клиента в Банк по телефону, Клиент предоставляет в Банк с письменное заявление об отзыве электронного документа, возврате (приостановлении движения) денежных средств и блокировании доступа к Системе, а так же о компрометации идентификационной информации для доступа в Систему. Примерная форма заявления приведена в Приложении № 1 к настоящему Регламенту.

2.1.5. При отсутствии возможности выполнения условий п. 2.1.4. Клиент незамедлительно отправляет сканированную копию заявления в Банк по факсу или по электронной почте и по телефону извещает Банк об отправке.

2.1.6. Клиент должен представить в Банк оригинал заявления, указанного в п 2.1.4. в срок не более 2 (Двух) рабочих дней с момента отправки в Банк сканированной копии заявления.

2.1.7. Клиент обеспечивает сохранность (целостность) ЭУ, поместив его в место с ограниченным доступом, обеспечив при этом защиту от вскрытия (стикеры, наклейки, пластилин и т.п.) и по возможности фиксирует их фотографированием со всех ракурсов. Если позволяют размеры ЭУ, следует поместить его в непрозрачный пакет (мешок) и опечатать горловину.

2.1.8. Клиенту рекомендуется проинформировать все банки, с которыми он имеет договорные отношения, и предусматривающие использование системы дистанционного банковского обслуживания, о факте хищения денежных средств и обратиться с просьбой о внеплановой замене ключевой и/или идентификационной информации.

2.1.9. Клиенту рекомендуется, по возможности, оперативно обратиться с письменным заявлением к своему Интернет-провайдеру (Приложение № 5 к настоящему Регламенту) для получения в электронной форме журналов соединений с Интернет с электронного устройства Клиента или из его ЛВС как минимум за три месяца, предшествовавшие факту хищения денежных средств.

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

2.2. В случае хищения денежных средств:

2.2.1. Клиент готовит объяснения о значимых действиях и событиях, в том числе действия с ЭУ, используемыми для работы в Системе, предшествовавших факту хищения денежных средств, об использовании ЭУ в целях, отличных от осуществления операций в системе ДБО, посещаемых сайтах, замеченных 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.

2.2.2. Клиент в срок не более 2 (Двух) календарных дней с момента выявления им хищения денежных средств обращается с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств (глава 21 УК РФ) Примерная форма заявления Клиента в правоохранительные органы приведена в Приложении № 6 к настоящему Регламенту.

2.2.3. Клиент в срок не более 2 (Двух) рабочих дней обращается в суд с исковым заявлением в отношении получателя денежных средств (указав все известные реквизиты получателя) о взыскании неосновательно полученного обогащения и процентов за пользование денежными средствами (глава 60 ГК РФ), а также с ходатайством о принятии судом мер по обеспечению иска в виде ареста денежных средств на счете получателя в сумме неосновательно полученного обогащения. К исковому заявлению необходимо приложить

копию заявления о возбуждении уголовного дела либо копию талона КУСП, содержащую отметку правоохранительного органа о его приеме.

2.2.4. В срок, не превышающий 3 (Трех) рабочих дней с момента обращения в правоохранительные органы и суд (отсчет ведется от события, наступившего последним) Клиент предоставляет в Банк копии следующих документов:

- Копию объяснения о значимых действиях и событиях в соответствии с п. 2.2.1. настоящего Регламента;
- Копию искового заявления в суд с отметкой о принятии;
- Копию заявления о возбуждении уголовного дела, либо копию талона КУСП, содержащую отметку правоохранительного органа о его приеме.

2.2.5. Одновременно с копиями документов, указанных в п. 2.2.4. настоящего Регламента, Клиент предоставляет в Банк Справку по факту инцидента информационной безопасности в Системе (Приложение № 2 к настоящему Регламенту).

3. Последовательность действий сотрудников Банка:

3.1. При получении телефонного обращения Клиента о приостановке исполнения (блокировании) ЭД, сотрудники Банка должны немедленно предпринять разумно возможные и достаточные действия для идентификации Клиента, в том числе, посредством использования контактной информации, указанной в Договоре.

3.2. При подтверждении обращения незамедлительно принять меры к приостановке дальнейшей обработки ЭД.

3.3. При невозможности аутентификации Клиента, зафиксировать данный факт, и продолжить обработку ЭД, если нет иных оснований для приостановки дальнейшей обработки электронного документа.

3.4. В случае завершения обработки ЭД незамедлительно в любой доступной форме направить в службу безопасности банка получателя несанкционированного платежа/перевода информацию о факте хищения денежных средств с просьбой о приостановке обработки ЭД (о приостановке зачисления средств на счет получателя).

3.5. Оперативно направить с использованием сервисов расчетной системы Банка России или по системе SWIFT в банк получателя денежных средств сообщение с просьбой о приостановлении зачисления средств на счет получателя и возврате средств (Приложение № 7 к настоящему Регламенту).

3.6. Оперативно направить письмо в банк получателя или к оператору платежной системы по факту хищения денежных средств (Приложение № 8 к настоящему Регламенту) с просьбой о прекращении обработки ЭД, блокировке Системы и платежных карт клиента – получателя, применении к получателю платежа мер контроля в рамках системы ПОД/ФТ и возврате средств.

3.7. Истребовать у Клиента подтверждение о подаче им заявления в правоохранительные органы и получить его копию в срок не более 3 (Трех) рабочих дней со дня получения обращения Клиента в Банк о факте хищения денежных средств.

3.8. Подготовить документы, указанные в Приложении № 4 к настоящему Регламенту.

3.9. Осуществить силами ответственных структурных подразделений Банка либо с привлечением организаций, предоставляющих квалифицированные услуги по расследованию инцидентов информационной безопасности, по меньшей мере, следующие действия:

3.9.1. Получить от ответственных сотрудников Банка, обслуживающих Систему, администраторов сети и т.д. экспертные заключения в рамках их компетенции по корректности идентификационной информации Клиента в Системе, корректности формирования ЭД, целостности и авторства ЭД.

3.9.2. Провести анализ собранной информации с целью выявления источника осуществления хищения денежных средств и возможной причастности сотрудников Банка. Результаты проверки оформить документально.

3.9.3. При необходимости – провести технические мероприятия, направленные на предотвращение сокрытия следов, уничтожения информации и т.д., для чего задействовать используемые в Банке средства и методы защиты информации.

3.9.4. Обеспечить хранение собранной информации в неизменном виде для передачи правоохранительным органам по запросу.

3.9.5. При необходимости провести, документально зафиксировав полученные результаты, следующие проверочные мероприятия в целях формирования необходимой доказательной базы по факту хищения денежных средств:

3.9.5.1. Найти оспариваемый Клиентом ЭД в базе данных Системы и в базе данных автоматизированной банковской системы (далее – АБС) Банка.

3.9.5.2. Если оспариваемый ЭД не найден в базе данных Системы, но имеется в базе данных АБС Банка:

3.9.5.2.1. По журналам систем ДБО и АБС установить, присутствовал ли оспариваемый Клиентом ЭД в Системе ранее.

3.9.5.2.2. В свойствах ЭД установить его авторство, дату, время и способ его создания.

3.9.5.2.3. Получить объяснения от своих работников, уполномоченных на оформление и проверку ЭД (электронных платежных документов), администраторов Системы и АБС Банка, включая администраторов безопасности систем.

3.9.5.2.4. Провести 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, штатно допущенных к управлению Системы, и средств удалённого управления указанными рабочими станциями.

3.9.5.2.5. Получить записи систем видеонаблюдения, управления доступом в помещения и т.д.

3.9.5.2.6. Оценить возможность продолжения эксплуатации Системы.

3.9.5.3. Если ЭД найден в базе данных Системы, проверить подлинность оспариваемого ЭД.

3.9.5.4. Если подлинность Электронного платежного документа не установлена:

3.9.5.5. Получить объяснения от работников Банка, уполномоченных на оформление и проверку электронных платежных документов, поступивших по Системе, администраторов Системы и АБС Банка, администраторов безопасности ДБО и АБС Банка (другого уполномоченного лица).

3.9.5.6. По журналам Системы установить, была ли подлинность ЭД утрачена в процессе эксплуатации Системы, а также оценить возможность продолжения эксплуатации Системы.

3.9.6. Если подлинность ЭД установлена:

3.9.6.1. Получить от уполномоченного работника Банка журналы работы Системы и проанализировать их на предмет наличия записей, содержащих признаки несанкционированного доступа посторонних лиц.

3.9.6.2. Сохранить на съемном носителе журналы работы Клиента в Системе.

3.9.6.3. Провести мероприятия, направленные на обеспечение целостности носителя.

3.9.6.4. Провести анализ информации с целью выявления возможной причастности к хищению денежных средств сотрудников Банка. Результаты проверки оформить документально. При необходимости провести технические мероприятия, направленные на предотвращение сокрытия следов хищения.

3.9.6.5. Получить от Клиента Справку по факту инцидента информационной безопасности в Системе (Приложение № 2 к настоящему Регламенту).

3.9.6.6. На основании собранной информации оформить и передать в правоохранительный орган, осуществляющий расследование по факту хищения денежных средств, объяснение по факту хищения денежных средств (Приложение № 8 к настоящему

Регламенту). В случае отказа клиента от обращения в правоохранительные органы оформить обращение по факту хищения денежных средств в региональное подразделение МВД от имени Банка по форме, приведенной в Приложении № 9 к настоящему Регламенту.

3.9.6.7. Обратиться в БСТМ МВД России либо его региональное отделение с заявлением об оказании содействия в расследовании факта хищения денежных средств с подробным описанием обстоятельств его совершения (Приложение № 10 к настоящему Регламенту) и по запросу БСТМ МВД России направить документы, указанные в Приложении № 4 к настоящему Регламенту.

3.9.6.8. В случае хищения денежных средств Клиента, по счетам которого зафиксированы поступления средств бюджета любого уровня, также направить информационное письмо на имя руководителя ФСБ России о факте хищения денежных средств с подробным описанием обстоятельств его совершения (Приложение № 11 к настоящему Регламенту) и по запросу ФСБ России направить документы, указанные в Приложении № 4 к настоящему Регламенту.

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

Приложение № 1.1

к Регламенту взаимодействия Клиента и Банка в случае выявления хищения или подозрения на хищение денежных средств Клиента в системе «ТКВ Express»

ФОРМА ЗАЯВЛЕНИЯ КЛИЕНТА В БАНК ОБ ОТЗЫВЕ ПЛАТЕЖА, ВОЗВРАТЕ ДЕНЕЖНЫХ СРЕДСТВ И БЛОКИРОВАНИИ ДОСТУПА К СИСТЕМЕ «ТКВ Express»

Председателю Правления
ТКБ БАНК ПАО
Ивановскому Е. Л.

от _____
ФИО заявителя

проживающего: _____
адрес места жительства

паспорт: №_____ серия_____ выдан _____
дата выдачи

_____
кем выдан

контактный телефон: __(_____)_____
телефон заявителя

адрес для корреспонденции _____
почтовый адрес

Уважаемый Евгений Леонидович!

«___» _____ 20___ года с моего банковского счета, открытого в Вашем Банке, по системе дистанционного банковского обслуживания «ТКВ Express» были похищены денежные средства, которые, по имеющейся у меня информации были переведены со следующими реквизитами платежа:

Дата платежа: _____
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 мою учетную запись в системе «ТКВ Express», провести процедуру компрометации используемых мною средств доступа и оказать содействие в возврате денежных средств.

_____ _____
подпись расшифровка подписи

«___» _____ 20__

Примечание: Если какие – либо данные платежа отсутствуют, оставьте соответствующие им поля не заполненными.

Приложение № 1.2

к Регламенту взаимодействия Клиента и Банка в случае выявления хищения или подозрения на хищение денежных средств Клиента в системе «ТКВ Express»

ФОРМА СПРАВКИ ПО ФАКТУ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ДБО «ТКВ Express»

Идентификатор Клиента_____

№ телефона сотовой связи Клиента +7 (___)___-__-__

«___» _____ 20__ неустановленным лицом через систему ДБО «ТКВ Express» была совершена несанкционированная операция по переводу денежных средств со следующими реквизитами:

Дата платежа: _____
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: _____[1]

Дополнительно сообщаю:

Количество ЭУ, настроенных для доступа в Систему: _____.

Для доступа в Систему хотя бы раз использовались

☐ корпоративные ЭУ
☐ личные ЭУ
☐ ЭУ, находящиеся в общественном пользовании

Периодичность смены пароля системы ДБО: _____

Применяемые элементы безопасности ЭУ включают:

☐ соблюден порядок подготовки ЭУ к установке системы ДБО
☐ используется только программное обеспечение для работы системы ДБО
☐ 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 ключевые носители
☐ передача файлов и обмен сообщениями электронной почты на ЭУ ограничены
☐ целостность исполняемых файлов и файлов конфигураций контролируется с периодичностью _____
☐ используются средства сетевой защиты: _____
☐ на ЭУ запрещены входящие соединения из сети Интернет
☐ 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

[1] Для случаев перевода электронных денежных средств – указать реквизиты перевода.

☐ обеспечивается возможность доступа к ключевым носителям только уполномоченных лиц

Иная информация, имеющая отношение к инциденту: _____
_____
_____

_____ _____
подпись плательщика

☐ Я намерен обратиться в правоохранительные органы по факту хищения денежных средств.

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

и зарегистрировано за № _____ в КУСП

☐ Я не намерен обращаться в правоохранительные органы по факту хищения денежных средств.

О необходимости предоставления доступа сотрудников правоохранительных органов к электронному устройству, об ответственности за использование нелицензированного и контрафактного программного обеспечения предупрежден.

Заявитель: _____/_____/

Дата: _____/Телефон: _____

Приложение № 1.3

к Регламенту взаимодействия Клиента и Банка в случае выявления хищения или подозрения на хищение денежных средств Клиента в системе «ТКВ Express»

ФОРМА ЗАЯВЛЕНИЯ КЛИЕНТА В БАНК ПОЛУЧАТЕЛЯ ИЛИ К ОПЕРАТОРУ ПЛАТЕЖНОЙ СИСТЕМЫ О ПРИОСТАНОВЛЕНИИ ПЛАТЕЖА И ВОЗВРАТЕ ДЕНЕЖНЫХ СРЕДСТВ

Председателю Правления
ТКБ БАНК ПАО
Ивановскому Е. Л.

от _____
ФИО заявителя

проживающего: _____
адрес места жительства

паспорт: №_____ серия_____ выдан _____
дата выдачи

_____
кем выдан

контактный телефон: __(_____)_____
телефон заявителя

адрес для корреспонденции _____
почтовый адрес

Уважаемый Евгений Леонидович!

«____» _____ 20___ года с моего банковского счета были похищены денежные средства, которые, по информации, полученной из банка, были переведены со следующим реквизитам платежа:

Дата платежа: _____
Номер распоряжения: _____
Наименование банка плательщика: ТКБ БАНК ПАО
Наименование плательщика: _____
ИНН плательщика: _____
Номер счета плательщика: _____
Наименование банка получателя: _____
Наименование получателя: _____
ИНН получателя: _____
Номер счета получателя: _____
Сумма платежа: _____
Назначение платежа: _____[2]

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

_____ _____
подпись расшифровка подписи

«___» _____ 20__

[2] Для случаев перевода электронных денежных средств – указать реквизиты перевода.

Приложение № 1.4

к Регламенту взаимодействия Клиента и Банка в случае выявления хищения или подозрения на хищение денежных средств Клиента в системе «ТКВ Express»

ПЕРЕЧЕНЬ ДОКУМЕНТОВ В ОТНОШЕНИИ ПОТЕРПЕВШЕГО ФИЗИЧЕСКОГО ЛИЦА И (ИЛИ) ФИЗИЧЕСКОГО ЛИЦА, НА СЧЕТ КОТОРОГО НЕПРАВОМЕРНО ЗАЧИСЛЕНЫ ДЕНЕЖНЫЕ СРЕДСТВА

1. Договоры на открытие и обслуживание банковских счетов, договоры о предоставлении услуг и подключении Клиента к «Системе».
2. Сведения о точном месте открытия и месте нахождения счета физического лица.
3. Сведения о паспортных данных физического лица (в том числе копия паспорта и иного удостоверения личности – при наличии).
4. Технический носитель информации, содержащий записи видеокамер, имеющие отношение к хищению (до процессуального изъятия оригинала технического носителя информации следует обеспечить сохранность записей).
5. Документы, отражающие статистику соединений с системой электронных расчетов банка посредством «Системы», с указанием учетных записей, внешних IP-адресов клиента и точного времени соединений в период осуществления несанкционированного перевода.
6. Журналы авторизации по электронным средствам платежа в банкоматах, данные о телефонах и адресах электронной почты, на которые было настроено оповещение об инцидентах, номера телефонов и адреса электронной почты, с которых поступали сообщения мошенников (при наличии), данные, указанные на подложных сайтах (при наличии).
7. Сведения о подключенных уведомительных услугах банка (СМС-уведомление, голосовая авторизация, уведомление на электронную почту, привязка к выделенному IP-адресу и других имеющихся услугах) с приложением копий документов, акцептованных банком при предоставлении указанных услуг.
8. Материалы, подготовленные службой безопасности банка по итогам проведения внутренних проверок.

Приложение № 1.5

к Регламенту взаимодействия Клиента и Банка в случае выявления хищения или подозрения на хищение денежных средств Клиента в системе «ТКВ Express»

ФОРМА ПИСЬМА ИНТЕРНЕТ ПРОВАЙДЕРУ О ПРЕДОСТАВЛЕНИИ ЖУРНАЛОВ СОЕДИНЕНИЙ (ЛОГОВ)

от _____
должность, ФИО заявителя

проживающего: _____
адрес места жительства

паспорт: _____
номер паспорта, дата выдачи, кем и когда выдан

контактный телефон: _____
телефон заявителя

адрес для корреспонденции _____
почтовый адрес

Уважаемый (ая) _____
имя, отчество руководителя

«____» _____ 20___ года в ___:___ по *московскому* времени со счета _____ по системе дистанционного банковского обслуживания (ДБО) был осуществлен несанкционированный перевод денежных средств. Компьютер, с которого обычно осуществляется подключение к системе ДБО, располагается по адресу _____.

Вероятной причиной несанкционированного перевода могло послужить заражение компьютера вредоносным программным обеспечением или кража средств доступа в систему.

«____» _____ 20__ года между _____ и вами был заключен договор № _____ об оказании _____ услуг.

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

_____ _____
подпись расшифровка подписи

«___» _____ 20__

Приложение № 1.6

к Регламенту взаимодействия Клиента и Банка в случае выявления хищения или подозрения на хищение денежных средств Клиента в системе «ТКВ Express»

ФОРМА ЗАЯВЛЕНИЯ КЛИЕНТА В ПРАВООХРАНИТЕЛЬНЫЕ ОРГАНЫ О ВОЗБУЖДЕНИИ УГОЛОВНОГО ДЕЛА ПО ФАКТУ ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ

Начальнику ОВД по _____
наименование ОВД

от _____
должность, ФИО заявителя

проживающего: _____
адрес места жительства

паспорт: _____,
номер паспорта, дата выдачи, кем и когда выдан

место работы _____
наименование организации

контактный телефон: _____
телефон заявителя

адрес для корреспонденции _____
почтовый адрес

ЗАЯВЛЕНИЕ

Прошу провести проверку настоящего заявления по факту незаконного завладения принадлежащими _____
ФИО потерпевшего

денежными средствами (кражи) с использованием системы дистанционного банковского обслуживания **«ТКВ Express»** банка ТКБ БАНК ПАО

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

Дата платежа: _____

Номер распоряжения: _____

Наименование банка плательщика: ТКБ БАНК ПАО

Наименование плательщика: _____

ИНН плательщика: _____

Номер счета плательщика: _____

Наименование банка получателя: _____

Наименование получателя: _____

ИНН получателя: _____

Номер счета получателя: _____

Сумма платежа: _____

Назначение платежа: _____[3].

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.

[3] Для случаев перевода электронных денежных средств – указать реквизиты перевода.

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

Факт появления этого перевода был установлен «____» _____ 201__ г.

_____

ФИО лица, установившего факт несанкционированного перевода, должность, наименование организации

при _____.

обстоятельства обнаружения факта несанкционированного перевода

Электронное устройство, с которого осуществляется подключение к системе ДБО, располагается по адресу _____, доступ к электронному устройству ограничен, прямая кража реквизитов доступа (учетной записи, пароля) маловероятна.

Вероятной причиной этого несанкционированного перевода 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.

_____ _____
подпись расшифровка подписи

«___» _____ 20__ г.

Приложение № 1.7

к Регламенту взаимодействия Клиента и Банка в случае выявления хищения или подозрения на хищение денежных средств Клиента в системе «ТКВ Express»

ФОРМА СООБЩЕНИЯ В БАНК ПОЛУЧАТЕЛЯ ПО СИСТЕМЕ SWIFT О ПРИОСТАНОВЛЕНИИ ПЛАТЕЖА И ВОЗВРАТЕ ДЕНЕЖНЫХ СРЕДСТВ

(оформляется в виде сообщения свободного формата системы SWIFT (MT199) с соблюдением принятых в системе правил транслитерации.)

Поле «20» сообщения должно содержать подстроку «FRAUD»
Поле «79» сообщения должно содержать текст, аналогичный приведенному ниже:

UVAJAEMYE KOLLEGI, _____BANK PROSIT VAS OKAZATX SODEiSTVIE V BLOKIROVKE I VOZVRATE NESANKCIONIROVANNO SPISANNYH DENEJNYH SREDSTV NA OSNOVANII ZAYAVLENIa KLIENTA PO P/P __ OT _____ NA SUMMU _____ RUB. NAQ DEBET _____ PLATELXqIK _____ VAQ KREDIT _____ POLUcATELX _____. PROSIM VAS VERNUTX NESANKCIONIROVANNO SPISANNUu SUMMU PO SLEDUuqIM REKVIZITAM: _____ BANK BIK _____ K/ScET _____ R/ScET _____ POLUcATELX - _____ V SLUcAE NEVOZMOJNOSTI VOZVRATA INFORMIRUiTE NAS O PRIcINE OTKAZA S UKAZANIEM DANNYH POLUcATELa SWIFT SOOBqENIEM PISXMOM PO FAKSU _____ I PO BANKOVSKOi POcTE.
S UVAJENIEM, _____ TEL.(___) _____

Приложение № 1.8

к Регламенту взаимодействия Клиента и Банка в случае выявления хищения или подозрения на хищение денежных средств Клиента в системе «ТКВ Express»

ФОРМА ПИСЬМА БАНКА ПЛАТЕЛЬЩИКА В БАНК ПОЛУЧАТЕЛЯ ИЛИ К ОПЕРАТОРУ ПЛАТЕЖНОЙ СИСТЕМЫ ПО ФАКТУ ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ

_____
должность руководителя

_____
наименование организации

_____
Фамилия И.О.

Уважаемый (ая) _____!
имя, отчество руководителя

«____» _____ 20___ года с банковского счета нашего клиента, открытого в нашем банке, были переведены денежные средства на счет Вашего клиента со следующими реквизитами платежа:

Дата платежа: _____
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: _____[4]

В связи с тем, что наш клиент заявил о хищении денежных средств, просим Вас приостановить прохождение платежа, блокировать систему ДБО и платежные карты Вашего клиента – получателя, применить к получателю платежа мер контроля в рамках системы ПОД/ФТ в связи с совершением операции, в отношении которой возникают подозрения в ее совершении в целях отмывания доходов, полученных преступным путем, или финансирования терроризма, зачислить указанную в сообщении сумму на счет 47416 «Суммы, поступившие на корреспондентские счета до выяснения» и осуществить мероприятия в порядке, предусмотренном пунктом 4.67 Положения от 16 июля 2012 г. № 385–П «О Правилах ведения бухгалтерского учета в кредитных организациях, расположенных на территории Российской Федерации».

Просим Вас также в соответствии с п.1.7 ст.6 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» сообщить информацию о паспортных данных и месте нахождения получателя платежа, в целях исполнения статей 6 и 131 ГПК РФ, а также статьи 7 Федерального конституционного закона от 31.12.1996 №1-ФКЗ «О судебной системе Российской Федерации» и статьи 19 Конституции Российской Федерации, для предъявления ему судебного иска.

_____ _____ _____
должность подпись расшифровка подписи

«___» _____ 20__

Исп. _____
Фамилия И.О.

тел. _____

[4] Для случаев перевода электронных денежных средств – указать реквизиты перевода.

Приложение № 1.9

к Регламенту взаимодействия Клиента и Банка в случае выявления хищения или подозрения на хищение денежных средств Клиента в системе «ТКВ Express»

ФОРМА ОБЪЯСНЕНИЯ БАНКА ПЛАТЕЛЬЩИКА ПО ФАКТУ ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ

ОБЪЯСНЕНИЕ

г. _____ «__» _____201__ г.
время ___ ч. ___ мин.

Оперуполномоченный _____
_____
получил объяснение от гр. _____
1. Фамилия, имя, отчество _____
2. Год рождения _____
3. Место рождения _____
4. Образование _____
5. Национальность _____
6. Гражданство _____
7. Место работы, должность или род занятий _____
_____
8. Место жительства _____
9. Сведения о паспорте _____
_____

На русском языке разговариваю свободно. В услугах переводчика не нуждаюсь, ст. 51 Конституции РФ мне разъяснена и понятна. _____

По существу заданных мне вопросов могу показать следующее.

Я, _____ работаю в _____
ФИО наименование банка

(Банк) в должности _____.
должность

_____
наименование клиента

является Клиентом системы дистанционного банковского обслуживания (ДБО) нашего Банка. Реквизиты Клиента:

_____
ИНН; место нахождения/адрес регистрации и паспортные данные; почтовый адрес; контактные телефоны

_____

_____

_____

«___» _____ 20__ Клиент представил в Банк заявление, оспаривающее правомерность проведения Банком платежа со следующими реквизитами:

Дата платежа: _____
Номер распоряжения: _____
Наименование банка плательщика: _____
Наименование плательщика: _____
ИНН плательщика: _____
Номер счета плательщика: _____

Наименование получателя: _____
ИНН получателя: _____
Номер счета получателя: _____
Сумма платежа: _____
Назначение платежа: _____[5]

Указанный платеж проведен Банком на основании распоряжения, полученного Банком по системе ДБО. Клиент утверждает, что оснований для данного денежного перевода нет, поскольку с получателем платежа у него отсутствуют договорные и иные деловые отношения, равно как и какие-либо обязательства перед ним. Оспариваемый перевод Клиент расценивает как хищение принадлежащих ему денежных средств.

По факту оспоренного Клиентом перевода сообщаю следующее:

1. Оспоренное распоряжение получено по системе ДБО
2. Дата и время получения распоряжения: ___ч. ___ мин. «___» _____ 20__
3. Для получения доступа в систему ДБО использовались корректные реквизиты Клиента: _____
   перечислить: логин, пароль, одноразовый пароль с карты/СМС/брелока и т.п.
4. распоряжение содержит корректные электронные подписи (ЭП) Клиента в количестве _____ штук, определенном договором с Клиентом
5. ЭП Клиента являются действующими, оснований для отказа в исполнении ПП Банком не было
6. Используемый при совершении оспоренного платежа IP, MAC адреса _____
   IP и MAC адреса с указанием: использовались / не использовались Клиентом ранее
7. Аналогичные IP и MAC адреса при подключении других Клиентов _____
   зафиксированы / не зафиксированы
8. Использованные для подтверждения оспоренного Клиентом платежа пароли и криптографические ключи вырабатывались __ _____
   Клиентом / Банком
9. Сотрудники Банка доступ к электронным устройствам, с которых осуществлялась работа Клиента с системой ДБО _____
   имели / не имели

Иные существенные обстоятельства инцидента:

_____

_____

На основании изложенного считаю, что создание оспоренного платежа сотрудниками Банка _____
возможно / маловероятно / невозможно

Объяснение получил: о\у _____

[5] Для случаев перевода электронных денежных средств – указать реквизиты перевода.

Приложение № 1.10

к Регламенту взаимодействия Клиента и Банка в случае выявления хищения или подозрения на хищение денежных средств Клиента в системе «TKB Express»

ФОРМА ЗАЯВЛЕНИЯ БАНКА ПЛАТЕЛЬЩИКА В МВД РОССИИ ОБ ОКАЗАНИИ СОДЕЙСТВИЯ В РАССЛЕДОВАНИИ ФАКТА ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ

Начальнику

Бюро специальных технических мероприятий МВД России

_____
(звание)

_____
(Фамилия И.О.)

119049, Москва, ул. Житная, д. 16

О предоставлении информации

Уважаемый _____!
(Имя Отчество)

«____» _____ 20___ года с банковского счета нашего клиента, открытого в нашем банке, были переведены денежные средства со следующими реквизитами платежа:

Дата платежа: _____
Номер распоряжения: _____
Наименование банка плательщика: _____
Наименование плательщика: _____
ИНН плательщика: _____
Номер счета плательщика: _____
Наименование получателя: _____
ИНН получателя: _____
Номер счета получателя: _____
Сумма платежа: _____
Назначение платежа: _____[6]

Клиент обратился в Банк с заявлением о хищении денежных средств.

Инцидент произошел в результате получения доступа к счетам Клиента с использованием электронной системы дистанционного банковского обслуживания.

Клиент обратился в ОВД _____
район, округ, город, субъект федерации и иные идентифицирующие ОВД данные

[6] Для случаев перевода электронных денежных средств – указать реквизиты перевода.

по месту регистрации. Заявление зарегистрировано за № _____ в КУСП.

Указанные противоправные действия совершены с использованием информационных технологий. Проблема хищения денежных средств со счетов клиентов банка посредством информационных технологий касается не только защиты законных интересов отдельных клиентов, но и затрагивает безопасность государства в кредитно-финансовой сфере, выявляет слабые звенья в противодействии посягательствам на общественные отношения, охраняемые законом, в частности, отношения в сфере компьютерной информации, что может привести к дестабилизации национальной платежной системы Российской Федерации.

Просим Вас оказать содействие в розыске и привлечении к ответственности лиц, совершивших незаконные действия в отношении Клиента нашего Банка.

Для сведения и оперативного взаимодействия Банк готов направить все имеющиеся материалы по указанному инциденту.

_____ _____ _____
должность подпись расшифровка подписи

«___» _____ 20__

Исп. _____
Фамилия И.О.

тел. _____

Приложение № 1.11

к Регламенту взаимодействия Клиента и Банка в случае выявления хищения или подозрения на хищение денежных средств Клиента в системе «ТКВ Express»

ФОРМА ИНФОРМАЦИОННОГО ПИСЬМА БАНКА ПЛАТЕЛЬЩИКА В ФСБ РОССИИ О ФАКТЕ ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ

Директору Федеральной службы безопасности России,

_____

(звание)

_____

(Фамилия И.О.)

107031, ул.Большая Лубянка, дом 1/3

О факте хищения денежных средств

Уважаемый _____!
(Имя Отчество)

ТКБ БАНК ПАО настоящим письмом информирует о противоправных действиях по отношению к Клиенту нашего Банка с использованием компьютерных технологий, в результате которых произошло хищение денежных средств.

«____» _____ 20___ года с банковского счета нашего Клиента, открытого в нашем Банке, были переведены денежные средства со следующими реквизитами платежа:

Дата платежа: _____
Номер распоряжения: _____
Наименование банка плательщика: _____
Наименование плательщика: _____
ИНН плательщика: _____
Номер счета плательщика: _____
Наименование получателя: _____
ИНН получателя: _____
Номер счета получателя: _____
Сумма платежа: _____
Назначение платежа: _____[7]

Согласно имеющейся информации, на счету клиента находились/могли находиться бюджетные средства.

Клиент обратился в ОВД _____
район, округ, город, субъект федерации и иные идентифицирующие ОВД данные

по месту регистрации. Заявление зарегистрировано за № ___ в КУСП).

Хищение денежных средств со счета клиента банка посредством компьютерных технологий касается не только защиты законных интересов отдельного клиента, но и затрагивает безопасность государства в кредитно-финансовой и бюджетной сфере, выявляет слабые звенья в противодействии

[7] Для случаев перевода электронных денежных средств – указать реквизиты перевода.

посягательствам на совершение преступления в сфере охраняемой законом компьютерной информации, что может привести к дестабилизации как бюджетной, так и национальной платежной системы Российской Федерации.

Для сведения и оперативного взаимодействия Банк готов направить имеющиеся материалы по инциденту.

_____ _____ _____

должность подпись расшифровка подписи

«___» _____ 20__

Исп. _____

Фамилия И.О.

тел. _____

Перечень приложений:

1. Приложение № 1.1. Форма заявления Клиента в Банк об отзыве платежа, возврате денежных средств и блокирования доступа к системе «ТКВ Express».
2. Приложение № 1.2. Форма Справки по факту инцидента информационной безопасности в системе ДБО «ТКВ Express».
3. Приложение № 1.3. Форма заявления Клиента в банк получателя или к оператору платежной системы о приостановлении платежа и возврате денежных средств.
4. Приложение № 1.4. Перечень документов в отношении потерпевшего физического лица и (или) физического лица, на счет которого неправомерно зачислены денежные средства.
5. Приложение № 1.5. Форма письма Интернет провайдеру ФОРМА о предоставлении журналов соединений (логов).
6. Приложение № 1.6. Форма заявления Клиента в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств.
7. Приложение № 1.7. Форма сообщения в банк получателя по системе SWIFT о приостановлении платежа и возврате денежных средств.
8. Приложение № 1.8. Форма письма банка плательщика в банк получателя или к оператору платежной системы по факту хищения денежных средств.
9. Приложение № 1.9. Форма объяснения банка плательщика по факту хищения денежных средств.
10. Приложение № 1.10. Форма заявления банка плательщика в МВД России об оказании содействия в расследовании факта хищения денежных средств.
11. Приложение № 1.11. Форма информационного письма банка плательщика в ФСБ России о факте хищения денежных средств.

Приложение № 2

к Договору на обслуживание Клиента - физического лица с использованием системы «ТКВ Express» № _____

от « ___ » _____ 20 г.

В ТКБ БАНК ПАО

от _____
(Фамилия)

_____
(Имя Отчество)

Паспорт: серия_____ номер_____

Выдан _____
(Кем)

_____

_____/_____/_____
(Когда)

Место жительства (регистрации):

_____

_____

ФОРМА

Заявление на разблокировку доступа к системе «ТКВ Express»

Я_____

Прошу разблокировать доступ в систему «ТКВ Express», заблокированный ранее по причине_____

_____20___г.

С взиманием комиссии, установленной действующими Тарифами Банка за разблокировку системы «ТКВ Express», ознакомлен и согласен.

Клиент														
Ф.И.О.		Подпись		Дата			/			/				

Заявление принял (заполняется сотрудником Банка)														
Заявление принял ФИО		Подпись		Дата			/			/				

Разблокировку системы «ТКВ Express» произвел (заполняется сотрудником Банка)														
Разблокировку произвел ФИО		Подпись		Дата			/			/				

БАНК КЛИЕНТ

_____ _____

М. П. (Ф.И.О., подпись)