Приложение № 7
к Правилам об использовании электронного
средства платежа Система «IBank»

ПОЛОЖЕНИЕ
о порядке действий сторон в случае компрометации средства подтверждения

1. События, которые могут быть расценены как компрометация Средства подтверждения:

   1.1. утрата/хищение Средства подтверждения;

   1.2. несанкционированное копирование ключа ЭП;

   1.3. передача ключа ЭП по открытым каналам связи;

   1.4. случаи, когда нельзя достоверно установить, что произошло со Средством подтверждения (в том числе случаи, когда Средство подтверждения вышло из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника);

   1.5. любые другие признаки осуществления несанкционированных действий в системе «IBank».

2. Решение о компрометации Средства подтверждения принимается владельцем ключа ЭП.

3. В случае компрометации Средства подтверждения и обнаружения факта несанкционированного списания средств Клиенту необходимо:

   3.1. немедленно прекратить любые действия с рабочим местом Системы «IBank», обесточить его и отключить от информационных сетей или перевести в режим гибернации;

   3.2. произвести фотосъемку Рабочего места, обеспечить его сохранность, поместив в место с ограниченным доступом и обеспечив при этом защиту от вскрытия. При необходимости - задействовать другое Рабочее место;

   3.3. обратиться в Банк с уведомлением о компрометации Средства подтверждения по форме Приложения № 8 не позднее дня, следующего за днем получения уведомления о совершенной операции, и просьбой заблокировать указанные Средства подтверждения и остановить обработку ЭД, подписанных/подтвержденных указанными Средства подтверждения;

   3.4. обратиться в иные банки, которые предоставляют Клиенту услуги электронного банкинга, с просьбой о внеплановой замене ключей ЭП в их информационных системах;

   3.5. предпринять меры для обеспечения сохранности и неизменности записей со средств обеспечения доступа в сеть Интернет за максимальный период времени;

   3.6. обратиться с письменным заявлением к своему Интернет-провайдеру или оператору связи для получения в электронной форме журналов соединений Рабочего места или локальной вычислительной сети Клиента с сетью Интернет;

   3.7. не предпринимать никаких действий для поиска и удаления компьютерных вирусов, восстановления работоспособности Рабочего места, не отправлять Рабочее место в сервисные службы для восстановления работоспособности;

   3.8. зафиксировать в протокольной форме значимые действия и события, предпринимаемые действия с Рабочим местом, подготовить объяснения в случае использования Рабочего места в целях, отличных от осуществления операций в системе электронного банкинга, посещаемых сайтах, перебоях в работе или отказах Рабочего места, обращениях в службы сопровождения, в Банк, о сторонних лицах, побывавших в месте расположения Рабочего места и т.д.

   3.9. все действия с Рабочим местом протоколировать и документировать, в том числе с использованием фотосъемки.

   В случае компрометации Средства подтверждения, если факт несанкционированного списания средств не обнаружен, Клиенту необходимо:

   3.10. обратиться в Банк с уведомлением о компрометации Средства подтверждения по форме Приложения № 8 не позднее дня, следующего за днем обнаружения факта компрометации, и просьбой заблокировать указанные Средства подтверждения и остановить обработку ЭД, подтвержденных указанными Средствами подтверждения.

4. О компрометации ключа ЭП Клиент уведомляет Банк следующими способами:

4.1. по телефону, указанному на Сайте Банка. Клиент уведомляет сотрудника службы технической поддержки Банка, при этом идентификация Клиента осуществляется по Блокировочному слову. Клиент заполняет Уведомление о прекращении действия средства подтверждения и(или) об утрате средства подтверждения и (или) об использовании ЭСП без согласия Клиента по утвержденной форме (далее - Уведомление) и незамедлительно отправляет его в Банк. Банк незамедлительно, но не позднее 1 часа с момента обращения Клиента по телефону и подтверждения его полномочий, останавливает обработку ЭД, подписанных указанными ключами ЭП, и блокирует указанные ключи ЭП на срок не более 4 часов. В случае неполучения Банком от Клиента в указанный срок оригинала Уведомления, Банк имеет право любым способом запросить у Клиента подтверждение факта обращения в Банк и/или продолжить обработку ЭД, подписанных указанными ключами ЭП, и/или разблокировать указанные Клиентом ключи ЭП.

4.2. по электронной почте. Клиент заполняет Уведомление и отправляет скан-копию Уведомления на электронную почту Help@kremlinbank.ru. Клиент незамедлительно отправляет оригинал Уведомления в Банк. Банк незамедлительно, но не позднее 1 часа с момента получения скан-копии Уведомления останавливает обработку ЭД, подписанных указанным в Уведомлении ключом ЭП, и блокирует указанные ключи ЭП на срок не более 8 часов. В случае неполучения Банком от Клиента в указанный срок оригинала Уведомления, Банк имеет право любым способом запросить у Клиента подтверждение факта обращения в Банк и/или продолжить обработку ЭД, подписанных указанными ключами ЭП, и/или разблокировать указанные Клиентом ключи ЭП.

4.3. Клиент передает оригинал Уведомления в отделение Банка, в котором обслуживается. Банк незамедлительно, но не позднее дня, следующего за днем получения оригинала Уведомления, останавливает обработку ЭД, подписанных указанным в Уведомлении ключом ЭП, и блокирует указанные ключи ЭП. При наличии технической возможности, Банк может исполнить указанное уведомление в более короткий срок.

5. Электронные документы, находящиеся на момент получения/исполнения Уведомления в статусе «На обработке» / «На исполнении» отзыву не подлежат.