Приложение №2
к Условиям дистанционного банковского обслуживания
физических лиц в «Банк Кремлевский» ООО

ПРАВИЛА
безопасности при работе в системе дистанционного банковского обслуживания физических лиц «Интернет-банк/Мобильный банк»

1. ОБЕСПЕЧЬТЕ БЕЗОПАСНОСТЬ УСТРОЙСТВА ДОСТУПА, С ИСПОЛЬЗОВАНИЕМ КОТОРОГО ОСУЩЕСТВЛЯЕТСЯ РАБОТА В СИСТЕМЕ «ИНТЕРНЕТ-БАНК/МОБИЛЬНЫЙ БАНК»

1.1. Перед входом в Систему необходимо удостовериться в том, что на Устройстве доступа, с использованием которого осуществляется работа в Системе, установлено, активировано и работает современное лицензионное антивирусное программное обеспечение, регулярно обновляются его антивирусные базы. Регулярное обновление антивирусных баз и проведение антивирусных проверок позволит Вам существенно снизить вероятность заражения Вашего Устройства вредоносными программами (особенно важно контролировать обновление, если нет постоянного подключения к сети Интернет). Если существуют подозрения или основания считать, что данное Устройство доступа может быть заражено вирусами – не осуществляйте с него работу в Системе.

1.2. На Устройстве доступа рекомендуется использовать только лицензионное программное обеспечение, регулярно устанавливать рекомендуемые производителями обновления, как операционной системы, так и прикладного программного обеспечения (в том числе браузера, PDF-ридера, Flash-плеера), это позволит своевременно устранить выявленные уязвимости. Обновления следует устанавливать только из доверенных источников (с официального сайта производителя).

1.3. Рекомендуется использовать на вашем Устройстве доступа персональный межсетевой экран для входа в Интернет. Это позволит значительно снизить риск удаленного управления злоумышленниками из сети Интернет и локальной сети вашим Устройством доступа и кражи конфиденциальной информации. Дополнительно в настройках персонального межсетевого экрана рекомендуется разрешить подключение вашего Устройства доступа только к северу Системы (https://elf.faktura.ru/elf/app/?site=kremlevsky) и серверам обновлений разработчиков программного обеспечения, любые иные подключения рекомендуется запретить.

1.4. Рекомендуется осуществлять работу с Системой с использованием отдельной учетной записи в операционной системе Устройства доступа, защищенной сложным паролем, известным только Вам (см рекомендации в п.3.3 настоящих Правил). Права пользователя в операционной системе Устройства должны быть минимально необходимыми, должна быть запрещена установка прикладного программного обеспечения за исключением необходимого для работы в Системе.

1.5. Рекомендуется избегать работы в Системе с использованием «недоверенных» Устройств доступа, таких как компьютеры в интернет-кафе или другие общедоступные устройства, «чужие» устройства, временно используемые вами и т.п. Крайне нежелательна работа с Системой из публичных беспроводных сетей (например, бесплатный Wi-Fi и т.п.), вместо этого лучше воспользуйтесь «мобильным интернетом» (GPRS / EDGE / HSPA / 3G / LTE соединение). В вышеописанных случаях существенно повышается риск кражи Ваших конфиденциальных данных и денежных средств. Если же данные рекомендации не могут быть Вами выполнены, то при первой же возможности измените пароль, войдя в Систему с «доверенного» Устройства доступа.

1.6. Не оставляйте без присмотра Ваше Устройство доступа с активной сессией работы в Системе, блокируйте доступ к Устройству при помощи пароля на время Вашего отсутствия.

1.7. По возможности исключите посещение с Устройства доступа потенциально опасных Интернет-ресурсов (социальные сети, форумы, чаты, телефонные сервисы, файлообменные сервисы и т.д.), а также работу с почтовыми сообщениями, полученными из недостоверных источников.

2. ВЫПОЛНЯЙТЕ ПРАВИЛА БЕЗОПАСНОСТИ ПРИ РАБОТЕ В СИСТЕМЕ «ИНТЕРНЕТ-БАНК»

2.1. Перед введением логина и пароля при входе в Систему убедитесь, что соединение установлено именно со стартовой страницы Системы и в адресной строке web-браузера отображается «https://elf.faktura.ru/elf/app/?site=kremlevsky». Злоумышленники могут создать мошеннический ресурс со сходным адресом и визуально похожим на сайт Системы интерфейсом. Если Вы заметили, что адрес сайта отличается или есть иные признаки, вызывающие подозрения подлинности сайта (например, сообщение web-браузера о перенаправлении на другой сайт), не вводите никакой конфиденциальной информации и незамедлительно сообщите о данном факте по телефону Банка 8(499)241-88-14. Рекомендуется вводить адрес Системы только вручную в новом окне web-браузера в адресной строке и НЕ переходить на данную страницу по ссылкам из Интернет-ресурсов (за исключением www.kremlinbank.ru) или из e-mail / SMS-сообщений, даже если они отправлены от имени Банка.

2.2. При работе с Системой для обеспечения конфиденциальности между Банком и Вашим Устройством

доступа все данные передаются в зашифрованном виде. Перед началом работы в Системе необходимо удостовериться, что соединение установлено в защищенном режиме SSL. В префиксе в адресной строке web-браузера должен появиться символ S - https://.....ru, а так же отобразится иконка «закрытый замок» (может отличаться для разных web-браузеров). Расположение иконки зависит от версии web-браузера, но как правило «закрытый замок» располагается в конце правой части адресной строки, либо в правом нижнем углу экрана. При клике на данное изображение должны отображаться сведения о SSL-сертификате (в строке «кем выдан» должно быть указано Thawte SSL CA)

2.3. После окончания работы в Системе обязательно завершайте сеанс работы с Системой с помощью кнопки «Выход» (в правом верхнем углу экрана).

2.4. При вводе логина и пароля в Системе рекомендуется использовать виртуальную клавиатуру. Использование виртуальной клавиатуры обезопасит Вас от кражи конфиденциальных данных в случае заражения Вашего Устройства доступа вредоносным программным обеспечением.

2.5. Контролируйте состояние Ваших счетов. Регулярно проверяйте в Системе (особенно перед проведением операции) разделы «История операций» (история операций и платежей, совершенных в Системе), раздел «Шаблоны» (перечень сохраненных шаблонов операций). В случае, если Вы обнаружили операции, которые Вы не выполняли; шаблоны, которые Вы не создавали, незамедлительно заблокируйте Вашу учетную запись в Системе. Вы можете сделать это, связавшись с Банком по телефону 8(499)241-88-14, или самостоятельно в Системе.

3. СОБЛЮДАЙТЕ ПРАВИЛА БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ПАРОЛЕЙ, ОДНОРАЗОВЫХ SMS-ПАРОЛЕЙ, ОДНОРАЗОВЫХ КОДОВ

3.1. Правила безопасности при использовании одноразовых SMS-паролей:

3.1.1. Для повышения уровня безопасности рекомендуется исключить работу с Системой через мобильные устройства (смартфоны), на телефонные номера которых настроено SMS-информирование с одноразовыми паролями. Эта мера значительно усложнит кражу денежных средств при заражении вирусом Вашего мобильного устройства.

3.1.2. Не используйте для получения одноразовых SMS-паролей не принадлежащие Вам мобильные устройства и телефонные номера.

3.1.3. Никогда не оставляйте без присмотра и не передавайте третьим лицам мобильные устройства, используемые Вами для получения одноразовых SMS-паролей.

3.1.4. Запрещается хранение на мобильном устройстве (в напоминаниях, SMS и т.п.) логина и пароля для входа в Систему. В случае хищения мобильного устройства или его заражения вирусом злоумышленники могут получить доступ к этой информации.

3.1.5. В случае потери (кражи) мобильного устройства или смены телефонного номера, на который приходят SMS-пароли, необходимо незамедлительно обратиться в Банк по телефону 8(499)241-88-14 для блокировки учетной записи. В случае потери/кражи устройства также необходимо обратиться к оператору сотовой связи для блокировки SIM-карты.

3.1.6. Не используйте возможности переадресации или хранения архива СМС-сообщений в личном кабинете оператора связи.

3.1.7. Устанавливайте сложные пароли в личном кабинете оператора связи. Данная мера позволит уменьшить риски несанкционированного подключения услуги переадресации SMS-сообщений на телефонные номера злоумышленников и последующего перехвата одноразового пароля.

3.1.8. Рекомендуем обратиться к оператору связи и заблокировать выполнение каких-либо действий с Вашей SIM-картой по доверенности. Это не позволит злоумышленником переоформить на третье лицо Ваш телефонный номер по поддельной или недействительной доверенности.

3.1.9. В случае если у Вас без видимых на то причин перестала работать SIM-карта («сеть не найдена») необходимо незамедлительно обратиться за разъяснениями к оператору связи. В данном случае возможно мошенничество с использованием копии Вашей SIM-карты.

3.2. Правила безопасности при использовании push-уведомлений:

3.2.1. Одноразовые пароли посредством push-уведомлений доставляются только на одно доверенное устройство. Устройство становится доверенным только при подтверждении в мобильном банке, установленном на этом устройстве.

3.2.2. Если используется функция быстрого входа с помощью PIN-кода, периодически меняйте его на новый. Не рекомендуется использовать код, который совпадает с каким-либо используемым в другом сервисе, устройстве или приложении.

3.2.3. Если используется функция быстрого входа с помощью отпечатков пальцев, периодически проверяйте настройки своего устройства на предмет регистрации чужих отпечатков.

3.2.4. Помните, что одноразовые push-уведомления не сохраняются в истории сообщений и автоматически подставляется в поле для ввод одноразового пароля.

3.3. Дополнительные рекомендации для владельцев смартфонов:

3.3.1. Установите пароль на доступ к Вашему мобильному устройству. Используйте сложный пароль или пин-код. Средства блокировки по простому графическому ключу или фотографии не обеспечивают должного уровня защиты.

3.3.2. Не используйте мобильные устройства с расширенными правами (Jailbreak, Root или иные операции, не поддерживаемые официально производителями).

3.3.3. Установите на Вашем мобильном устройстве и регулярно обновляйте мобильный антивирус (рекомендуется использовать антивирус российского производителя, так как он учитывает региональную специфику вредоносного ПО).

3.3.4. Своевременно устанавливайте обновления для Вашего мобильного устройства и установленных на нем приложений. Установку производите только из доверенных источников (Google Play Market и Apple AppStore, маркеты производителей устройств и т.п.). Иные способы установки приложений и обновлений небезопасны. Недопустима установка или обновление приложений по ссылке в e-mail / SMS-сообщении от имени Банка. Обратите внимание: Банк никогда не высылает писем и SMS-сообщений с прямыми ссылками на установку или обновление приложений.

3.3.5. При установке на Ваше мобильное устройство дополнительного программного обеспечения обращайте внимание на полномочия, которые необходимы программе. Не допускайте установки программ, которым требуются излишние полномочия, особенно в части чтения и отправки SMS-сообщений, доступа к сети Интернет, клавиатуре и т.п. Установку производите только из проверенных и надежных источников (Google Play Market и Apple appStore и т.п.). При наличии технической возможности рекомендуется включить на мобильном устройстве режим установки только подписанных приложений с проверкой сертификата. Не устанавливайте приложения по ссылкам, полученным от неизвестных Вам источников.

3.3.6. Если Вы заметили, что на Ваше мобильное устройство перестали приходить SMS, в том числе перестали приходить SMS-пароли от Банка, необходимо прекратить использование мобильного устройства. В данном случае возможно мошенничество с заражением Вашего мобильного устройства вирусом, перехватывающим SMS-сообщения. Для проверки рекомендуем установить SIM-карту в другое мобильное устройство, провести операцию в Системе и дождаться прихода SMS-пароля. Так же о заражении вирусом может свидетельствовать подозрительная работа устройства (самопроизвольные звонки и рассылки SMS, несанкционированная загрузка и установка программного обеспечения). В случае выявления данных фактов рекомендуем обратиться за помощью в службу технической поддержки производителя Вашего мобильного устройства.

3.4. Правила выбора и хранения пароля для входа в Систему:

3.4.1. Для работы с Системой необходимо использовать только сложные пароли, удовлетворяющие следующим требованиям:

3.4.1.1. пароль должен иметь длину от 8 до 20 символов, в нем должно быть не менее двух цифр и двух букв, допускается использование букв латинского алфавита, цифр, знаков !#$%&()*+-./:;<=>?[\, используйте буквы верхнего и нижнего регистра;

3.4.1.2. обратите внимание, что регистр и язык букв пароля имеет значение;

3.4.1.3. пароль не должен содержать последовательности одинаковых символов и групп символов, легко угадываемые комбинации символов (dddddd, 333444555, qwerty, 12345, abc123 и т.п.);

3.4.1.4. пароль не должен содержать связанных с Вами данных (имена и даты рождения членов семьи, адреса, телефоны, часть номера банковской карты и т.п.);

3.4.1.5. пароль не должен содержать словарных слов (password, football, русские слова, набранные в английской кодировке, например, gfhjkm – пароль);

3.4.1.6. пароль не должен совпадать с шестью предыдущими паролями и не должен совпадать с именем входа;

3.4.1.7. пароль не должен быть копией или комбинаций паролей, используемых Вами в других системах или Интернет-ресурсах (операционная система Устройства, электронная почта, социальные сети, развлекательный ресурсы в сети Интернет и т.п.).

3.4.2. Никогда не сообщайте свой пароль третьим лицам, в том числе родственникам и сотрудникам Банка, вводите пароль только при работе в Системе. Помните, что сотрудник Банка не имеет права запрашивать у Вас пароль, даже если Вы самостоятельно обратились в Банк. Вводите пароль только в Системе, Банк никогда не отправляет сообщений с просьбой уточнить или предоставить пароль.

3.4.3. Не записывайте и не храните пароль в местах доступа третьих лиц. Запрещается хранить пароль на Устройстве доступа, мобильном устройстве, используемом для получения одноразовых SMS паролей, а также на иных электронных носителях, доступ к которым могут получить третьи лица.

3.4.4. Рекомендуется осуществлять смену пароля доступа к Системе не реже одного раза в 12 месяцев.

3.4.5. При возникновении подозрений, что Ваш пароль стал известен третьим лицам, необходимо незамедлительно сменить пароль или заблокировать доступ в Систему, обратившись в Банк по телефону 8(499)241-88-14, либо самостоятельно заблокировать доступ в Системе.

4. ОСТЕРЕГАЙТЕСЬ МОШЕННИЧЕСТВА

4.1. Банк никогда не связывается по телефону и не осуществляет рассылок сообщений по SMS или e-mail с просьбой предоставить, подтвердить или уточнить Вашу конфиденциальную информацию (пароли, логины, кодовое слово, Ф.И.О., паспортные данные, номер мобильного телефона, на который приходят одноразовые пароли, параметры банковских карт и другие конфиденциальные данные). Не отвечайте на такие сообщения.

4.2. Банк никогда не связывается с просьбой установить или обновить программное обеспечение, в своих электронных письмах никогда не рассылает программы. Не открывайте подозрительные файлы, присланные Вам по электронной почте.

4.3. При получении подозрительного сообщения от имени Банка не отвечайте на него, не переходите по

ссылкам, указанным в подозрительном сообщении. Мошенники могу создать ресурсы в сети Интернет с адресами, похожими на адреса сайта Банка https://i.название.ru. В сообщениях Банка никогда не будет просьбы зайти в Систему по указанной в сообщении ссылке.

4.4. При работе с Системой обращайте внимание на страницу входа и интерфейс Системы. Если у Вас возникли подозрения в подлинности сайта, необходимо незамедлительно прекратить работу и связаться с Банком по телефону 8(499)241-88-14 (никогда не связывайтесь по телефону, указанному на подозрительной странице).

4.5. Для входа в Систему необходимо ввести логин и пароль (а в случае усиленного режима защиты дополнительно одноразовый пароль). Если Вам предлагается также заполнить иные поля (телефон, номер карты и т.п.) немедленно прекратите работу в Системе и сообщите об этом в Банк.

4.6. Банк никогда не запрашивает одноразовый пароль или пароль на вход в Систему для отмены операций. При вводе пароля Вы даете Банку право на проведение операции, отменить ее с помощью пароля нельзя.

4.7. Если Вы самостоятельно связались с Банком, сотрудники могут уточнить у Вас персональную информацию, но не имеют права запрашивать у Вас пароль на вход в Систему и одноразовый пароль.

4.8. Банк никогда не направляет сообщений о блокировке/разблокировке Вашей учетной записи в Системе. Сотрудники Банка никогда не связываются по телефону, чтобы сообщить о недоступности Системы вследствие проведения каких-либо регламентных работ. Если Вы получили подозрительное сообщение от имени Банка, либо с Вами связались по телефону с одной из просьб, перечисленных в данном разделе, то рекомендуется сообщить о данном факте в Банк по телефону 8(499)241-88-14 (никогда не связывайтесь с Банком по телефону, указанному в подозрительном сообщении).

4.9. Обращайте внимание на появление подозрительной активности на Вашем Устройстве доступа, например, самопроизвольные движение курсора на экране, набор текста и т.п.

4.10. Обращайте внимание на невозможность доступа к сайту Системы и нестабильную работу Системы («зависания») при нормальной работе других Интернет-ресурсов, а также на невозможность доступа к Системе по причине несовпадения логина и пароля (в случае корректного набора). Данные факты могут свидетельствовать о заражении Вашего Устройства доступа вредоносным программным обеспечением. Если зараженное устройство уже использовалось для доступа к Системе, то незамедлительно заблокируйте Вашу учетную запись в Системе. Вы можете сделать это по телефону 8(499)241-88-14, или самостоятельно в разделе Системы «Параметры безопасности» (при этом вход в Систему должен быть осуществлен с «доверенного» устройства).

4.11. В случае несанкционированного списания денежных средств, для опротестования спорной операции, проведенной Банком по документу, подписанному аналогом собственноручной подписи ДПАСП (далее - Спорная операция), необходимо до обращения в судебные органы подать в Банк письменное или электронное заявление по каналу обратной связи на сайте Банка (www.kremlinbank.ru) с изложением сути претензии и детальным описанием Спорной операции (далее – Претензия), при необходимости приложить документы и материалы, подтверждающие обоснованность Ваших требований (например, бумажная распечатка спорного ДПАСП и/или файл с ДПАСП).

4.12. В случае если опротестованная операция не совершалась ни Клиентом, ни его Представителем, а также имеются иные признаки незаконного завладения денежными средствами (кражи) с использованием Системы, то Вам рекомендуется оперативно обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств (глава 21 УК РФ). После чего предоставить в Банк копию заявления о возбуждении уголовного дела, либо копию талона-уведомления, подтверждающего непосредственное обращение в правоохранительные органы и содержащего порядковый номер из книги учета сообщений о преступлениях, содержащую отметку правоохранительного органа о его приеме.

В случае утраты, а также при возникновении подозрений, что Ваши логин и пароль, либо еще не введенные в Систему одноразовый код или SMS-пароль стали известны третьим лицам, (в том числе представившимся сотрудниками Банка) незамедлительно заблокируйте Вашу карты.

Помните, что Ваше оперативное обращение в Банк может предотвратить несанкционированное списание, либо приостановить списание денежных средств, снизив Ваши финансовые потери.