Ассоциация банков России
(Ассоциация «Россия»)

ПРЕЗИДЕНТ

119180, Москва, ул. Большая Якиманка, д.23
www.asros.ru
asros@asros.ru
т. 8-(495)-785-29-90

от 26.10.2018 № 02-05/816

На №_____от_____

Директору Департамента
информационной безопасности
Банка России

В.А. Уварову

Уважаемый Вадим Александрович!

Ассоциация банков России 12 октября 2018 года провела заседание Комитета по информационной безопасности, на котором обсуждались изменения в деятельности подразделений кибербезопасности банков в связи с вступлением в силу Федерального закона от 27.06.2018 № 167-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств».

Ассоциация «Россия» благодарит Вас за участие в дискуссии и выражает надежду на дальнейшее плодотворное сотрудничество по обсуждаемым вопросам.

По итогам заседания было принято решение о представлении в Банк России вопросов, имеющихся у членов Комитета, о порядке работы по противодействию переводам денежных средств без согласия клиента (свод вопросов прилагается).

Прошу Вас рассмотреть прилагаемые материалы и направить в Ассоциацию разъяснения в целях повышения уровня осведомленности кредитных организаций.

Приложение: вопросы кредитных организаций на 8 л. в 1 экз.

С уважением,

Г.И. Лунтовский

Жижанов Г.В.
8-499-678-30-13

Приложение к письму Ассоциации «Россия»
от 26.10.2018 № 02-05/816

1. Распространяются ли требования Закона на следующие виды операций:
   a. совершённые без использования электронного средства платежа;
   b. операции в сети интернет с использованием банковской карты;
   c. любые операции с использованием банковских карт, включая операции покупки и оплаты услуг;
   d. операции с использованием любых электронных средств платежей;
   e. операции снятия наличных;
   f. p2p операции;
   g. операции в финансовых институтах (так называемые операции «Quasi cash»)?
2. Относятся ли нормы статьи 8 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» (далее – Закон 161-ФЗ) в новой редакции, обязывающие банки проводить контроль переводов денежных средств на наличие признаков перевода денежных средств без согласия клиента, ко всем поступающим по системе ДБО документам, приводящим к списанию денежных средств с карт/счетов клиента, включая распоряжения по закрытию вкладов/счетов, покупки страховок и подобных документов? С какого дня начинается отсчет срока приостановления исполнения распоряжения, указанный в этой статье?
3. Относятся ли требования Закона ко всем операциям по платежным картам (торговый эквайринг, списания на основании распоряжений по оплате, оформленных клиентами в устройствах самообслуживания, и т.п.)? В технологиях ПС нет понятия «возобновить», есть только «одобрить» и «отклонить». Допустим ли в целях исполнения требований Закона отказ в исполнении распоряжения (авторизации операции), и обязан ли банк самостоятельно инициировать новое распоряжение от имени клиента в случае отсутствия подтверждения операции в течение двух дней? Возможно ли оговорить области применения соответствующих положений в зависимости от технологических особенностей операций по переводу денежных средств (например, ограничить только операциями в каналах ДБО и т.п.) или Банк России полагается на внесение платежными системами/банками изменений в имеющиеся технологии и процессы?
4. Учитывая, что Закон требует «приостановить исполнение распоряжения», но не отказать в приёме его к исполнению — каким образом должны реализовываться требования Закона в случае, если процедура расчётов не предусматривает «заморозки» («холдирования») средств на счёте клиента, а напротив, предполагает автоматическое и моментальное исполнение распоряжения клиента с немедленным списанием средств (и соответственно, немедленное наступление безотзывности перевода) сразу после приёма распоряжения к

исполнению (к примеру, при формировании распоряжения в системе дистанционного банковского обслуживания)?

5. Правильно ли трактовать норму п.9.1 ст.9 «В случаях выявления оператором по переводу денежных средств операций, соответствующих признакам осуществления перевода денежных средств без согласия клиента, оператор по переводу денежных средств приостанавливает использование клиентом электронного средства платежа и осуществляет в отношении уменьшения остатка электронных денежных средств плательщика действия, предусмотренные частями 5.1 - 5.3 статьи 8 настоящего Федерального закона» как требование немедленно при выявлении признаков перевода денежных средств без согласия клиента в одном из переводов полностью заблокировать электронное средство платежа – карту и/или ДБО? Или достаточно заблокировать возможность использования электронного средства платежа для выполнения аналогичных приостановленной операций по способу оплаты (например, интернет-эквайринг), цели платежа (например, оплата услуг) получателю и подобных критериев? Осуществляется ли приостановление использования клиентом только того ЭСП, при помощи которого составлено распоряжение в целях осуществления перевода, соответствующего признакам осуществления перевода денежных средств без согласия клиента, выявленная оператором по переводу денежных средств, или всех ЭСП, в том числе и тех, при помощи которых клиент может потенциально составить подобное распоряжение? В случае приостановления в соответствии с Законом использования токена, формируемого к банковской карте в системах Apple Pay, Google Pay, Samsung Pay, допустимо ли сохранение у клиента возможности проведения операции с использованием самой банковской карты?

6. Закон не определяет обязанности банков относительно распоряжения (операции) и электронного средства платежа при получении отказа клиента от распоряжения (операции). Правильно ли понимать, что распоряжение (операцию) банк должен отклонить, а в отношении электронного средства платежа банк самостоятельно устанавливает условия снятия ограничений в использовании или блокировки?

7. Сможет ли кредитная организация в договоре с клиентом предусмотреть дополнительный срок для приостановления исполнения распоряжения, если оно имеет признаки осуществления перевода денежных средств без согласия клиента, наряду со сроком, указанным в ч. 5.3. ст. 8 Закона 161-ФЗ? Наделяется ли кредитная организация правом продлить блокировку карты на срок более двух рабочих дней при наличии признаков, указывающих, что операция совершена без согласия клиента, и в случае неполучения уведомления от клиента? Вправе ли кредитная организация продлить блокировку ЭСП на срок более двух рабочих дней, если ЭСП было заблокировано кредитной организацией по другим критериям, не указанным в критериях Банка России, но реализуемых кредитной организацией для минимизации риска несанкционированных операций или как продуктовые настройки?

8. Означает ли «неполучение от клиента подтверждения» факт невозможности установления контакта с клиентом или это только информации о том, что операция совершена без его согласия? Должен ли банк пытаться ему дозвониться в течении двух дней? Обязан ли будет банк в случае претензии клиента подтверждать факт неуспешного дозвона документально? Какова позиция Банка России в этой связи в части незащищенности Законом банка получателя средств?

9. Если клиент пытается совершить операцию, банк ее приостанавливает на основании признаков, клиент пытается совершить еще несколько операций, банк с клиентом связаться не может. Значит ли это, что через 2 дня банк должен провести все эти операции?

10. Правильно ли понимать, что сообщать клиенту об исполнении распоряжения/возобновлении использования клиентом электронного средства платежа после получения от него соответствующего подтверждения возобновления оператор по переводу денежных средств не обязан?

11. Как должен реагировать банк в случае, если он выявил подозрительную операцию, связался с клиентом и озвучил риски, клиент подтвердил операцию, банк «незамедлительно возобновил» исполнение распоряжение, а через какое-то время клиент обращается в банк с уведомлением о совершении операции без его согласия?

12. Какой именно срок вкладывается в формулировку «незамедлительно», применяемую в Законе? Распространяется ли указанный срок на выходные и праздничные дни? Просьба дать разъяснения касательно незамедлительности.

13. Если на телефоне у клиента находится вирус, который скрывает смс (у клиента нет информации о совершении операции), проведение операции через 2 дня увеличит уровень фрода?

14. Закон не определяет требований к форме получения от клиента подтверждения распоряжения (операции) и требований по идентификации/аутентификации клиента при получении такого подтверждения. Предполагает ли Банк России нормировать процесс получения подтверждения?

15. В соответствии с п.2 ч.5.2 ст.8 Закона 161-ФЗ в новой редакции «оператор по переводу денежных средств после выполнения действий, предусмотренных частью 5.1. ст. 8 ФЗ № 161-ФЗ (в ред. ФЗ № 167-ФЗ), обязан предоставить клиенту информацию в том числе о рекомендациях по снижению рисков повторного осуществления перевода денежных средств без согласия клиента.». Будут ли Банком России определены возможные критерии рекомендаций по снижению рисков повторного осуществления операций перевода денежных средств без согласия клиента?

16. Обязан ли оператор по переводу денежных средств приостанавливать использование электронного средства платежа для клиента – юридического лица после выявления/получения информации оператором по переводу денежных средств об осуществлении операции по переводу денежных средств без согласия клиента? Какие предусмотрены сроки приостановления использования клиентом – юридическим лицом электронного средства платежа?

17. Учитывая, что Закон связывает возникновение обязанностей банка по приостановлению исполнения распоряжения с выявлением операции, соответствующей признакам осуществления перевода без согласия клиента, возникают ли указанные обязанности у банка в случае, если операция подпадает только под один признак из сформулированных Банком России?

18. На основании каких данных банку необходимо определять место совершения операции (п.2.1.2)?

19. На основании каких данных банк может определить нетипичное устройство, с которого осуществляется операция по переводу денежных средств (п. 2.1.3.)?

20. Как часто будет обновляться информация об актуальных признаках? Может ли банк блокировать платежи, которые не соответствуют этим признакам? Какие будут санкции, если платеж, соответствующий данным признакам, не будет остановлен/ подтвержден клиентом?

21. Планируется ли разработка методик, позволяющая банкам-плательщикам/банкам получателям по косвенным признакам самостоятельно распознавать, что данные средства перечисляются/поступают по переводам без согласия клиентов?

22. В соответствии с внесенным изменениями в статью 9 Закона 161-ФЗ часть 11.3.

«В случае представления в течение пяти рабочих дней со дня совершения оператором по переводу денежных средств, обслуживающим получателя средств, действий, предусмотренных частью 11.2. настоящей статьи, получателем средств документов, подтверждающих обоснованность получения переведенных денежных средств или электронных денежных средств, оператор по переводу денежных средств, обслуживающий получателя средств, обязан осуществить зачисление денежных средств на банковский счёт получателя средств или увеличение остатка электронных денежных средств получателя средств.»

Принимая во внимание, что получателем денежных средств по операции, совершенной без согласия клиента (ЮЛ - отправителя), как правило являются злоумышленники (дроп-фирма. компания однодневка, ИП-дроп и т.п.), требование представления документов фактически перекладывает представление доказательной базы обоснованности на сторону возможного мошенника. При этом не рассматривается участие ЮЛ - потерпевшего (клиента - отправителя) в обосновании своего несогласия с совершенной операцией. Существующая практика обращения в полицию, возбуждения уголовных дел, ареста денежных средств, постановлений суда и т.д. не укладывается в срок 5 дней, в течение которого (исходя из положений Закона) у потерпевшего фактически есть законное основание для возврата похищенных денежных средств. Будет ли подготовлен Банком России перечень документов, принимаемых банком в качестве доказательства обоснованности денежного перевода получателю (с требованием проведения оператором их правовой экспертизы, в т.ч. экспертизы на подлинность)? Каков механизм проверки

подлинности представленных документов? Какова позиция Банка России в части арбитража по полученным от клиента документам с точки зрения их легитимности и достаточности?

23. Какие действия банку следует предпринять в случае невозможности однозначно установить соответствие предоставленных получателем документов, подтверждающих обоснованность получения денежных средств, конкретному переводу (например, в реквизите «Назначение платежа» расчетного документа не указана информация, идентифицирующая документ (номер, дата))? Вправе ли кредитная организация определять в своих внутренних документах дополнительные основания приостановления исполнения распоряжения клиента в соответствии с установленной Законом процедурой?

24. Согласно п. 11.4 ст. 9 Закона 161-ФЗ при непредставлении в установленный срок (5 рабочих дней со дня направления обслуживающим банком уведомления) документов, подтверждающих обоснованность получения переведенных денежных средств или электронных денежных средств, обслуживающий получателя средств банк должен осуществить возврат денежных средств не позднее 2 рабочих дней после истечения пятидневного срока. В связи с чем просим уточнить, если документы, подтверждающие обоснованность получения переведенных денежных средств или электронных денежных средств, получены по истечении пятидневного срока, но до их возврата банку, обслуживающему плательщика средств, вправе ли банк, обслуживающий получателя средств, произвести их зачисление на счет получателя средств?

25. В законе отсутствует порядок действий участников расчетов (плательщика, банка плательщика, банка получателя, получателя) в ситуации, когда плательщик решил отозвать свое уведомление (предусмотренное ч. 11 ст. 9 Закона 161-ФЗ) в течение 5 рабочих дней, указанный в ч. 11.2 ст. 9 Закона № 161-ФЗ Может ли он это сделать? Что должен делать банк плательщика и банк получателя в таком случае? Как и в какой форме должен будет происходить документооборот в данном случае?

26. Какая форма и порядок отправки сообщения планируются Банком России для случаев уведомления банка получателя средств о приостановлении зачисления на банковский счет клиента в рамках исполнения требований частей 11.1-11.5, вводимых Законом. Планируется ли отправка таких сообщений в формате УФЭБС?

27. Какие именно требования имеются в виду в следующей формулировке: «Статья 57.4. Банк России по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, устанавливает обязательные для кредитных организаций требования к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента, за исключением

требований к обеспечению защиты информации, установленных федеральными законами и принятыми в соответствии с ними нормативными правовыми актами.»?

28. Может ли клиент-держатель платежной карты банка заранее дать согласие на исполнение всех операций по платежной карте, держателем которой он является, с целью освобождения оператора от обязанности приостанавливать исполнения распоряжений? Например, клиент активно путешествует и не желает, чтобы банк блокировал какие-либо его операции. То же самое касается клиентов – юридических лиц, обслуживающихся по системе Клиент-банк, которые приходят в банк и пишут заявление в произвольной форме об отказе от дополнительного подтверждения операций по их счету и просят, чтобы им не звонили.

29. Обязан ли оператор по переводу денежных средств, являясь банком получателя, осуществлять «мониторинг» входящих переводов до зачисления денежных средств на счет получателя, на предмет наличия признаков переводов, осуществлённых без согласия клиента? Например, получатель перевода (клиент банка получателя) указан в реестре Банк России «как подозрительный получатель». Вправе ли оператор по переводу денежных средств, в таком случае приостанавливать зачисление денежных средств на счет такого получателя, при условии, что от оператора по переводу денежных средств, обслуживающего плательщика, не поступило уведомление о приостановлении?

30. Оператор по переводу денежных средств в рамках реализуемой им системы управления рисками определяет в документах, регламентирующих процедуры управления рисками, процедуры выявления операций, соответствующих признакам осуществления переводов денежных средств без согласия клиента, на основе анализа характера, параметров и объема совершаемых его клиентами операций (осуществляемой клиентами деятельности). Требует ли данное положение документирование во внутренних документах организации правил определения подозрительных операций? Данные правила являются информацией ограниченного доступа и не раскрываются за пределами соответствующей функции, а соответственно должны предоставляться, например, в рамках проверки, регулятору.

31. Планируются ли какие-либо мероприятия для оперативного оповещения банков получателей средств по денежным переводам без согласия клиентов с учетом технологии обработки поступивших платежей в режиме он-лайн, при которой поступившие денежные средства зачисляются в автоматическом режиме в течение операционного дня по мере поступления электронных документов из Банка России, и клиенты могут оперативно их или снять или перевести в другой банк? В этом случае в банк получателя средств информация о переводе средств без согласия плательщика/запрос на приостановку зачисления средств на практике будет всегда поступать с опозданием. Будут ли рекомендованы Банком России какие-либо способы приостановки зачисления средств банком получателя для указанной технологии?

32. Существующие в настоящее время процедуры проверки операций в большинстве случаев обрабатываются автоматизировано системами мониторинга и

не предполагают непосредственную коммуникацию с клиентами для их подтверждения. Предполагают ли положения Закона обязательство банка осуществлять такую коммуникацию по каждой подозрительной операции?

33. Каким образом при обмене уведомлениями, запросами на отмену и при реализации процедуры возврата денежных средств банка плательщика и банка получателя должен осуществляться бухгалтерский учет денежных средств до момента наступления возврата/зачисления получателю? Каков код возврата при возврате денежных средств? Планируется ли Банком России выделение в списке счетов бухгалтерского учета целевого счета для учета средств в банке-получателе в случае незачисления средств на счет клиента в связи с получением уведомления об приостановлении зачисления средств? На каком счете должны учитываться денежные средства в банке получателя в течение 5 дней, приостановленные для зачисления на основании уведомления банка плательщика?

34. После внесения изменений остается проблема с тем, что после зачисления денежных средств на счет получателя в банке получателя эти денежные средства не могут быть возвращены. Могут ли банки, используя признаки подозрительных операций или специальные списки «неблагонадежных» клиентов, не зачислять денежные средства на счет получателя, а оставить их на счетах до выяснения (НВС)?

35. Денежные средства зачислены банком получателя на счет клиента, но в договоре с клиентом есть условие о праве банка списывать со счета клиента без его дополнительного распоряжения ошибочно зачисленные денежные средства. Почему Банк России считает, что при получении информации о том, что платежный документ плательщиком не составлялся (то есть деньги были зачислены в отсутствие надлежащего распоряжения плательщика – то есть ошибочно), банк получателя не может произвести такое списание (конечно в случае, если мошенник еще не успел увести деньги дальше)?

36. Что нужно считать расходами по расследованию инцидентов в соответствии с инструкцией Банка России № 4753-У?

37. Каким образом изменения, вносимые Законом, позволят бороться с дружественным фродом?

38. Спецификацию и описание как делать интеграцию с БД Финцерта для обязательных подтверждений операций по реквизитам/устройствам занесенных в БД необходимо получать через запрос в Банк России?

39. Какие уведомления (запросы) могут направляться через раздел «Другое» через АСОИ?

40. Какой формат вложений приоритетный – JSON/XLSX?

a. Формировать файлы формата JSON может только приложение «Инцидент ФинЦерт»?
b. Файлы формата XLSX формируются в соответствии с «Временным регламентом передачи данных…». К моменту

вступления в силу ФЗ взамен Временного регламента планируется выпуск документов.

c. Файлы формата XLSX использоваться не будут? Доработка внутренних систем планируется именно на формате XLSX.

41. Вопросы по документу «Признаки осуществления перевода денежных средств без согласия клиента» № ОД-2525:

a. Каким образом будет происходить обмен с базой данных?
b. Когда будет доступен регламент подключения?
c. Какая конкретная информация подпадает под «параметры устройства»?
d. Какие атрибуты понимаются под «обычно совершаемые клиентом»?