25 июля 2024 года вступил в силу Федеральный закон № 369-ФЗ от 24.07.2023 «О внесении изменений в Федеральный закон «О национальной платежной системе». Согласно новой редакции Федерального закона № 161-ФЗ «О национальной платежной системе» (далее - 161-ФЗ) у банков появились новые обязанности.

Банк «КУБ» (АО), как оператор по переводу денежных средств, обязан до списания денежных средств клиента осуществлять проверку наличия признаков осуществления перевода денежных средств без добровольного согласия клиента или с согласия клиента, полученного под влиянием обмана или при злоупотреблении доверием.

С 25 июля 2024 года действуют новые расширенные механизмы противодействия мошенническим операциям:

Платежи с использованием банковских карт, ЭДС или перевод по СБП

Банк отказывает в совершении операции по переводу денежных средств по подозрительным реквизитам из базы данных Банка России.

Если, несмотря на полученные предостережения от Банка, вы хотите совершить повторную операцию (содержащую те же реквизиты получателя и ту же сумму перевода), то при отсутствии иных установленных законодательством РФ оснований Банк принимает к исполнению распоряжение клиента, однако, если до проведения повторной операции Банк получил от Банка России информацию, содержащуюся в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, Банк отказывает в совершении операции в зависимости от способа перевода.

По истечении двух дней Вы можете осуществить действия по совершению последующей повторной операции. При отсутствии иных установленных законодательством РФ оснований Банк принимает к исполнению распоряжение клиента, однако если до проведения повторной операции Банк получил от Банка России информацию, содержащуюся в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, то Банк отказывает в совершении операции.

Безналичные переводы

Банк приостанавливает на 2 дня перевод денежных средств по подозрительным реквизитам, содержащимся в базе данных Банка России. Вы вправе подтвердить распоряжение не позднее одного дня, следующего за днем приостановления (при этом Банк вправе в дополнение запросить информацию, что перевод денежных средств не является переводом денежных средств без добровольного согласия).

При неполучении подтверждения и (или) информации, дополнительно запрошенной Банком, указанное распоряжение считается не принятым к исполнению.

При получении подтверждения распоряжения Банк принимает к исполнению подтвержденное распоряжение, однако, если до проведения операции Банк получил от Банка России информацию, содержащуюся в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, Банк приостанавливает прием к исполнению подтвержденного распоряжения клиента на 2 дня.

По истечении 2 дней Банк принимает к исполнению подтвержденное распоряжение.

Рекомендации по снижению рисков повторного осуществления перевода денежных средств без добровольного согласия клиента

1. Никому не сообщать одноразовый пароль, полученный от Банка в (SMS/push/и т.п.), реквизиты банковской карты.
2. Перед вводом учетных данных для доступа в ДБО на сайте Банка необходимо убедиться, что соединение установлено с официальным сайтом Банка. Для этого необходимо проверить правильность указания адреса сайта Банка в строке браузера и наличие сертификата безопасности (https в адресной строке).

3. При использовании для доступа к ДБО технического устройства, такого как компьютер, мобильное устройство (смартфон, планшет) рекомендуем:
    - использовать для доступа в ДБО только личные устройства;
    - включать на устройстве встроенные средства блокировки и разблокировки устройства входа в ДБО (логин/пароль для входа в ОС, логин/PIN-код/отпечаток пальца);
    - применять на устройстве лицензионные средства антивирусной защиты, обеспечить своевременную загрузку баз антивирусного программного обеспечения;
    - использовать на устройстве лицензионное программное обеспечение из доверенных источников (например, с сайтов разработчиков);
    - обеспечить на устройстве автоматическое обновление программного обеспечения;
    - использовать на устройстве учетные данные (логин) с правами администратора только при наличии существенной необходимости;
    - исключить возможность удаленного сетевого доступа к устройству, в том числе с помощью программ TeamViewer, AnyDesk, Ассистент и т.д., никому не направлять снимки и фотографии экрана;
    - исключить на устройстве посещение интернет-сайтов сомнительного содержания, загрузку и установку нелицензионного программного обеспечения;
    - не хранить на устройстве используемые для входа в ДБО учетные данные, в том числе в защищенных заметках, файлах, в записках под чехлами, на стикерах на мониторах и т.д.;
    - не открывать при работе на устройстве с электронной почтой письма, полученные от неизвестных источников, и особенно не открывать вложения и не переходить по ссылкам из таких писем;
    - по возможности использовать выделенное устройство входа в ДБО только для работы ДБО.

4. При использовании ключей для работы с системой «iBank2» рекомендуем:
    - никому не сообщать пароль от ключа электронной подписи системы «iBank2»;
    - не передавать ключи электронной подписи сотрудникам технической поддержки для проверки работы системы ДБО, проверки настроек взаимодействия с банком и т.п.;
    - при увольнении ответственного сотрудника, имевшего доступ к ключу электронной подписи, обязательно уведомить Банк о приостановлении использования электронного средства платежа