Меры безопасности при работе в системе ДБО
ООО РНКО «Платежный конструктор»

Вход в систему дистанционного банковского обслуживания (далее – ДБО) является многофакторным. Необходимо ввести Логин и Пароль. Не сообщайте никому свой Логин и Пароль доступа к системе ДБО. При попытке подключения к системе ДБО на Ваше мобильное устройство поступает уведомление для подтверждения входа. Если попытка входа осуществляется не Вами – не подтверждайте вход в систему ДБО. Сообщите об этом случае в РНКО по номерам телефонов, указанных на официальном сайте РНКО.

Используйте только доверенные компьютеры с лицензионным программным обеспечением. Регулярно обновляйте программное обеспечение.

Обязательно установите на компьютеры антивирусное программное обеспечение с ежедневным обновлением антивирусных баз. Выполняйте полную антивирусную проверку компьютера не реже одного раза в неделю.

Проверьте, что веб-адрес в адресной строке браузера начинается с «https». Иначе не входите в систему ДБО!

Клиент или работники клиента ни в коем случае не должны сообщать посторонним лицам информацию (например, логин и пароль доступа в систему ДБО, персональные данные, данные банковской карты, пароли из СМС и push-уведомлений, секретные слова и т.д.), использование которой посторонними лицами может привести к совершению перевода денежных средств без согласия клиента.

Каждый раз при входе в систему ДБО на номер мобильного телефона, указанный для уведомлений, поступает SMS сообщение с информацией об IP адресе, с которого проведено подключение. Имя отправителя сообщения «PaymentkitRU». Если предыдущий вход осуществлялся с другого IP адреса РНКО уведомляет об этом последующим SMS сообщением.

Каждый клиент РНКО может установить ограничения для входа в систему ДБО: указать страны, IP адреса, промежуток времени для возможного подключения и работы в системе ДБО. Для этого необходимо направить соответствующее сообщение в интерфейсе системы ДБО.

Клиент системы ДБО может установить ограничения по максимальной сумме одной операции и(или) операций за определенный период времени. Ограничения по операциям могут быть установлены как на все операции клиентов, так и в разрезе видов операций. Для этого необходимо направить соответствующее сообщение (заявление) в интерфейсе системы ДБО.

РНКО не запрашивает по телефону или электронной почте у своих клиентов информацию, связанную с персональными, авторотационными данными и различные одноразовые коды. Будьте

бдительны: не отвечайте на подобные запросы, злоумышленники могут представиться кем угодно!

При проведении операций в системе ДБО на мобильное устройство приходят уведомления с информацией об операции, внимательно проверяйте реквизиты получателя и суммы перед подтверждением отправки каждой операции.

Установите ограничение доступа на мобильное устройство (смартфон) используя ПИН-код, графический ключ, пароль или воспользуйтесь другой технологией ограничения доступа к устройству.

Система ДБО РНКО не применяет SMS с одноразовыми кодами для подтверждения платежа. Ни в коем случае не вводите и никому не сообщайте пришедший код, не подтверждайте операцию и обратитесь в РНКО о таких сообщениях.

Работники РНКО будут связываться с Вами в случае выявления признаков операций, относимых к операциям без согласия клиента (далее - ОБС). Виды таких операций определены требованиями федерального законодательства РФ и Банком России. Со стороны РНКО допустима приостановка ОБС на срок до двух дней, в течении которых Клиент должен подтвердить операцию или уведомить об ее отмене.

Не указывайте в социальных сетях и других открытых источниках абонентский номер мобильной связи, использующийся для уведомлений от системы ДБО.

В случае утери/кражи мобильного устройства, на котором установлена программа, применяемая для подтверждений входа и подтверждения операций в системе ДБО, немедленно сообщите об инциденте в РНКО.

Если вы сменили номер мобильной связи – обязательно сообщите об этом в РНКО.

Запишите контактный телефон для связи с РНКО. Если Вас просят связаться с РНКО по другому номеру, это может означать попытку мошенничества.

Устанавливайте любые мобильные приложения только из официальных магазинов приложений (play.google.com, apps.apple.com).