# ПАМЯТКА ДЛЯ КЛИЕНТОВ

**О действиях в случае обнаружения попытки или несанкционированного списания денежных средств в системе дистанционного банковского обслуживания (ДБО).**

В случае обнаружения несанкционированного доступа к счету и/или несанкционированного списания денежных средств со счета Банк рекомендует Клиенту осуществить следующие действия:

1. Немедленно обратиться на горячую линию клиентской службы по телефону 8(800) 550-51-37 с требованием о блокировке доступа Клиента к системе ДБО, приостановке исполнения платежа и/или просьбой оказания содействия в возврате несанкционированно списанных денежных средств.
2. Не позднее рабочего дня, следующего за днем устного обращения представить в Банк на официальный почтовый ящик ProstoBank@creditural.ru письменное заявление, заверенное печатью и подписью руководителя о факте несанкционированного списания с указанием даты, суммы платежа, других известных Клиенту обстоятельств, а также с просьбой оказания содействия в возврате несанкционированно списанных денежных средств.
3. Немедленно прекратить любые действия с электронными устройствами: персональный компьютер, ноутбук, планшетный компьютер и т.п., подключенным к системе ДБО, отключить его от сети и обесточить. Эти действия позволят предотвратить последующие инциденты, а также сохранить доказательства для проведения технической экспертизы.
4. Оперативно обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств. Копию заявления и талона - уведомления о его приеме предоставить на официальный почтовый ящик ProstoBank@creditural.ru срок не позднее 1 рабочего дня со дня выявления факта хищения денежных средств.
5. Для возобновления работы необходимо обратится в Банк для получения новых Одноразовых ключей (мобильного телефона, Авторизованного номера), регистрации нового Кодового слова или смены Авторизованного номера Клиента (также в случае замены SIM-карты при сохранении номера).
6. После окончания процедуры смены паролей не возобновлять деятельность на данной рабочей станции без проведения соответствующих технических мер, которые гарантируют полное уничтожение вирусных объектов, но только в том случае, когда уже не требуется сохранение доказательной базы в целях проведения расследования инцидента правоохранительными органами. В случае необходимости сохранения персонального компьютера в текущем состоянии, использовать в работе другой компьютер.