Об уголовной ответственности за хищение денежных средств с банковских карт.

С развитием информационных технологий появился особый вид криминальных посягательств, совершенных с использованием сети Интернета и коммуникационных устройств. На протяжении последних лет информационные технологии применяются при совершении хищений, связанных с посягательством на собственность государства, граждан и юридических лиц.На рост числа таких преступлений оказывает активное развитие новых форм платных услуг и сервисов, использование при расчетах цифровых средств платежей.

Уголовная ответственность за хищение денежных средств с банковской карты предусмотрена п. «г» ч. 3 ст. 158 УК РФ - кража, совершенная с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159.3 УК РФ). Для квалификации по этому пункту необходимо, чтобы действия виновного были тайными, то есть в отсутствие собственника, иных лиц либо незаметно для них. Если хищение с банковской карты совершено путем обмана или злоупотребления доверием, действия виновного квалифицируются по ст. 159 УК РФ (мошенничество).

Согласно п. 17 Постановления Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», в случаях когда лицо похитило безналичные денежные средства, воспользовавшись необходимой для получения доступа к ним конфиденциальной информацией держателя платежной карты (например, персональными данными владельца, данными платежной карты, контрольной информацией, паролями), переданной злоумышленнику самим держателем платежной карты под воздействием обмана или злоупотребления доверием, действия виновного квалифицируются как кража.

Хищение денежных средств с банковского счета, а равно в отношении электронных денежных средств возможно и путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, что является специальным видом мошенничества и влечет уголовную ответственность по п. «в» ч. 3 ст. 159.6 УК РФ.

Если для этого были созданы, использованы или распространены вредоносные компьютерные программы, действия виновного требуют дополнительной квалификации по ст. ст. 272, 273, 274.1 УК РФ.

Чтобы обезопасить себя от действий мошенников, необходимо придерживаться следующих рекомендаций:

- не сообщать конфиденциальные данные карты третьим лицам (срок, CVV-код и ПИН-код);

- подключить услугу СМС-уведомлений для контроля за счётом;

- ПИН-код хранить отдельно от карточки и прикрывать рукой клавиатуру банкомата или терминала в момент его ввода;

- установить расходные лимиты в интернет-банке или мобильном приложении;

- никогда никому не сообщать код из СМС для подтверждения операции, которую клиент не совершал (сотрудники банка не вправе запрашивать данную информацию);

- после выявления факта незаконного списания денег с карты необходимо срочно её заблокировать и обратиться в ближайшее отделение банка.

Соблюдение перечисленных мер безопасности любой поможет предотвратить нанесение ущерба от действий мошенников.