УДК 343.721 **Юридические науки**

Трубачев Никита Андреевич, *адъюнкт*

Дальневосточный юридический институт ДВЮИ МВД России

ПРОБЛЕМАТИКА РАСКРЫТИЯ ДИСТАНЦИОННЫХ МОШЕННИЧЕСТВ ОПЕРАТИВНЫМИ ПОДРАЗДЕЛЕНИЯМИ

Аннотация: Актуальность данного научного исследования заключается в непрерывном росте преступлений в сфере, связанной с дистанционным мошенничеством совершаемом при помощи информационно-телекоммуникационных технологий. В статье рассмотрены актуальная проблематика предотвращения и раскрытия преступлений, связанных с дистанционным мошенничеством, совершаемым при помощи информационно-телекоммуникационных технологий.

Ключевые слова: Дистанционное мошенничество. Сотовая связь. Банковские карты. Бесконтактный способ совершения преступления.

Annotation: The relevance of this scientific study lies in the continuous growth of crimes in the field of remote fraud committed using information and telecommunication technologies. The article deals with the actual problems of prevention and disclosure of crimes associated with remote fraud committed using information and telecommunication technologies.

Keywords: Remote fraud. Cellular. Bank cards. A contactless way of committing a crime.

Исследования аналитиков, в сфере, связанной с дистанционным мошенничеством совершаемом при помощи информационно-телекоммуникационных технологий, СберИндекса и IT-компании «Платформа ОФД» констатируют [1], что процент операций по безналичному расчету в

России в 2020 году достиг очередного исторического максимума, составив 54,1 %. Также данные свидетельствуют о том, что переводы граждан с карты на карту составили за 2020 год 44,8 трлн рублей, что на 25,8 % больше, чем за аналогичный период прошлого года. Кроме того, в ходе анализа статистических данных, предоставленных МВД России за 2020 год установлено, что на 77 % увеличилось количество преступлений, связанных с использованием информационных технологий по сравнению с АППГ [4].

Чрезвычайную актуальность данной проблемы демонстрирует факт того, что лицо совершившее данное преступление, может находиться в любой точке мира, конечно же, если оно имеет доступ к сети Интернет, и пользуется различными сервисами быстрого обмена сообщениями, типа WhatsApp, Telegram, Viber и т.д., в результате чего может получать доступ не только к банковским картам, путем взлома самого устройства, но и к иным особо охраняемым данным жертвы.

На сегодняшний день «изобретено» огромное количество способов оставить жертву без денежных средств на его банковском счете, из которых самые популярные: внедрение вредоносных программ на устройство пользователя; введение в заблуждение самой жертвы, путем использования психологических приемов и методов, таких как: представление мошенника сотрудником службы безопасности банка; кража денежных средств под предлогом выигрыша в конкурсе или проведения «фейковой» акции самим банком; рассылка СМС-сообщений о взломе банковской карты или банковского счета, способствовавшие в дальнейшей получению доступа к счету жертвы. В настоящее время, мошенничество с использованием банковских карт является чрезвычайно выгодным «бизнесом», причинами чего является элементарная не посвященность граждан Российской Федерации в способы и методы ведения такого вида преступной деятельности, излишняя доверчивость лицам, представляющимися «сотрудниками банковской организации», отсутствие средств у органов правопорядка для выявления таких лиц, а также сложность в поимке самого преступника, что говорит о трудности привлечения преступного

элемента к ответственности.

В ходе изучения практической деятельности оперативных подразделений было установлено, что в процессе расследования уголовного дела по факту совершения хищения с банковской карты потерпевшего, в случае, если у оперативного-подразделения имеются номера сотовых телефонов, с использованием которых совершались мошеннические действия или устанавливалась связь с жертвой и в ходе оперативно-розыскных мероприятий осуществляется установление конечного абонента сотовой связи (преступника), в результате чего становится известно, что номер принадлежит определенному оператору сотовой связи: «МТС», «Мегафон», «Билайн», а также субъект Российской Федерации, в котором данным номер зарегистрирован, но отсутствует ключевая информация о данных абонента или иные идентификационные сведения. Исходя из этого, предварительное расследование заходит «в тупик» и возможность дальнейшего расследования и установления преступника отсутствует.

В настоящее время преступниками разработано несколько десятков схем совершения подобных мошенничеств [2].

Важным обстоятельством при хищении с банковских карт граждан, является персонифицированность денежных средств, то есть движения денежных средств по банковским счетам отследить не представляет труда, поскольку каждое перемещение средств отражается в банковских документах что представляет определенную сложность для мошенников, в связи с чем перемещение денежных средств на карты преступников, является первоначальной стадией осуществления преступного замысла (одновременно, преступление является оконченным, так как имеется возможность распорядиться похищенным имуществом).

После получения преступниками денежных средств на используемый ими банковский счет (обычно, данный банковский счет также принадлежит не лицам, совершавшим преступление, он может быть куплен на «Даркнете» или получен иным путем), они немедленно пытаются их обналичить или перевести на иной

банковский счет или в криптовалюту. Например, при обналичивании денежных средств, существуют специальная сфера услуг, предоставляемая также в «Даркнете» по обналичиванию и передаче преступникам денежных средств. Также при переводе похищенных средств в криптовалюту, где теряется конкретная цепочка операций и установление пути перемещения денежных средств не представляется возможным.

При изучении научной литературы мы обратили внимание на рекомендации при проведении такого следственного действия, как допрос, где излагается, что необходимо выяснить у подозреваемого (допрашиваемого) лица следующие сведения: характер, способ хищения, время, какие устройства и абонентский номера сотового оператора использовались при осуществлении преступного замысла, после завладения денежными средствами, на какие банковские счета направлялись или каким способом и в каком месте обналичивались, каким образом была получена информация о банковских счетах и устройствах жертвы, использовалось ли антивирусное программное обеспечение и так далее. Но исходя из практической составляющей ОВД, в большинстве случаев местонахождение лица совершившего преступление установить не представляется возможным, а в случае установления лица, доказывание по данным преступлением имеет определенную сложность, так как обычно, данные лица имеют достаточный уровень юридической грамотности, и осознают, что ход предварительного расследования зависит от тех показаний, которых они дадут в ходе проведения допроса.

Но несмотря на вышесказанное уголовное законодательство защищает сферу банковских прав граждан, в результате чего может наступить ответственность за совершение преступлений, предусмотренных следующими статьями: 158, 159, 159.1, 159.2, 159.3, 159.5,159.6 [3]. Также Федеральным Законом от 23.04.2018 года № 111-ФЗ «О внесении изменений в уголовный кодекс Российской Федерации» усилена уголовная ответственность и введен в действие пункт «г», части 3, ст. 158 УК РФ – кража, совершенная с банковского счета, а равно в отношении электронных денежных средств (при отсутствии

признаков состава преступления, предусмотренного ст. 159.3 УК РФ). При квалификации по данному пункту, необходимо, чтобы действия виновного были тайными, то есть в отсутствии собственника или незаметно для него. Как показывает практика, совершение данного преступления происходит при следующих обстоятельствах: собственник утерял банковскую карту и лицо её нашедшее воспользовалось ей, используя систему бесконтактного платежа «Пай Пасс» (PayPass) услуг и товаров на сумму менее 1 000 рублей без введения пин-кода в соответствующий терминал или иное устройство принятия платежа.

Если хищение с банковской карты произведено путем обмана или злоупотребления доверием, данное деяние будет квалифицироваться как мошенничество по ст. 159 УК РФ. Конкретно способ совершения деяния разграничивает квалификацию данных преступлений.

В основном проблемы уголовной ответственности за совершение хищений с банковских карт заключаются в следующем:

1. Отсутствие возможности у сотрудников оперативных и следственных подразделений установления виновного лица и его местонахождения в связи с невозможностью установления конечного пользователя по абонентскому номеру телефона.
2. Сложность доказывания вины по данной категории преступлений.
3. Законодательные пробелы регулирующие технические операции по банковским картам.
4. Малая осведомленность населения о способах и методах совершения данного вида преступлений.

Для устранения условий способствовавших совершению данных преступлений, а также для наиболее эффективного расследования данной категории преступлений, мы предлагаем следующее решение данных проблем:

1. При оформлении сим-карты у конкретного оператора сотовой связи установить обязательную биометрическую систему идентификации личности и присвоить данные биометрии конкретной сим-карте, чтобы исключить пользование данной сим-картой иных пользователей. Применения данного

способа не составит труда, так как большинство современных устройств имеет функции идентификации личности путем отпечатка пальца или функции распознавания лица пользователя.

2. Исключить использование системы «PayPass» с функцией оплаты товаров и услуг до 1 000 рублей без введения пин-кода банковской карты. При каждой операции по банковской карте требовать обязательного введения пароля карты.

3. Необходимо проводить массовое оповещение граждан Российской Федерации о способах и методах совершения данной категории преступлений, в особенности в отношении лиц пожилого возраста.

Несмотря на действительно непрерывное развитие и совершенствование информационных технологий, а также выработку новых средств и методов ведения вышеупомянутой преступной деятельности, с данными преступлениями можно и нужно бороться, используя предложенные нами решения.

Библиографический список:

1. Сбербанк России. URL: https://www.sberbank.ru/ru/press_center/all/article?newsID=69f89a71-452a-47ac-8adf-b731d85a8e8c&blockID=1303&regionID=77&lang=ru&type=NEWS.

2. Мерецкий, Н. Е., Жердев П. А. Некоторые особенности хищений денежных средств со счетов граждан при использовании услуги «Мобильный банк» // Вестник Дальневосточного юридического института МВД России. 2017. N 3(40). с. 140–146.

3. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон от 29.11.2012 N 207-ФЗ (в ред. от 01.07.21) // Собрание законодательства РФ. 1996. N 25. Ст.2954.

4. Состояние преступности. URL: https://mvdmedia.ru/news/official/o-sostoyanii-prestupnosti-v-rossiyskoy-federatsii-po-itogam-8-mesyatsev-2020-goda/.