УДК 441.4

Даренский Р.Н.
Студент
2-го курса магистратуры юридического факультета
«Кубанский государственный аграрный университет им. И.Т. Трубилина»
г. Краснодар, РФ
Влезько Д.А., *кандидат юридических наук, доцент*
«Кубанский государственный аграрный университет им. И.Т. Трубилина»
г. Краснодар, РФ

ПРОБЛЕМЫ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ БАНКОВСКИХ КАРТ

Аннотация*: автором исследуются основные проблемы расследования мошенничества с использованием платежных средств, в том числе банковских карт. Проанализированы основные способы совершения данного преступления. Рассмотрена проблема квалификации мошенничества (ст. 159.3 УК РФ) и кражи с банковского счета (п. «г» ч. 3 ст. 158 УК РФ) на примере из судебной практики. Рассмотрены иные факторы, препятствующие расследованию мошенничества с использованием банковских карт. По результатам исследования предложены меры предупреждения совершения мошенничества с использованием банковских карт.*

Ключевые слова*: мошенничество, банковская карта, расследование, электронное средство платежа, хищение, банк.*

Abstract: the author examines the main problems of fraud investigation using means of payment, including bank cards. The main ways of committing this crime are analyzed. The problem of fraud qualification (Article 159.3 of the Criminal Code of the Russian Federation) and theft from a bank account (paragraph "d" of part 3 of Article 158 of the Criminal Code of the Russian

Federation) is considered using an example from judicial practice. Other factors hindering the investigation of fraud using bank cards are considered. According to the results of the study, measures have been proposed to prevent fraud using bank cards.

Keywords: fraud, bank card, investigation, electronic means of payment, theft, bank.

Мошенничество с использованием электронных средств платежа, в том числе с использованием банковских карт, с каждым годом совершается чаще. Данный факт объясним тем, что процент использования электронных платежных средств возрастает в связи с повсеместным внедрением безналичных расчетов в жизнь общества.

Согласно данным Центрального Банка Российской Федерации[1] на 01.01.2024 на территории государства количество платежных карт, эмитированных кредитными организациями, превышает 449 миллионов. Простота и удобство использования безналичного расчета привлекает не только добросовестных пользователей, но и лиц, имеющих корыстный умысел на завладение чужими денежными средствами.

Уголовная ответственность за совершение мошенничества с использованием банковских карт определена в ч. 1 ст. 159.3 УК РФ. Важным признаком объективной стороны данного деяния является совершение хищения путем обмана или злоупотребления доверием. Иначе говоря, способ совершения преступления, предусмотренного ч. 1 ст. 159.3 УК РФ заключается в том, что мошенник выдает себя за лицо, которое имеет право распоряжаться денежными средствами, связанными с банковской картой. В связи с этим, данный состав преступления важно уметь разграничивать с кражей, совершенной с банковского счета, ответственность за которую установлена п. «г» ч. 3 ст. 158 УК РФ.

Вследствие чего мы можем сделать вывод о том, что одной из проблем расследования мошенничества с использованием банковской карты является

трудность установления признаков объективной стороны в процессе квалификации преступления. По результатам изучения примеров из судебной практики, нами был сделан вывод о том, что сотрудниками органов предварительного расследования нередко определяется неверная квалификация деяния.

Так, например, Советским районным судом г. Омска первоначальная квалификация содеянного по п. «г» ч. 3 ст. 158 УК РФ была изменена на ч. 1 ст. 159.3 УК РФ [2]. Преступление было совершено посредством оплаты банковской картой, находящейся в незаконном владении Андреевой О.Н., ряда покупок в различных торговых павильонах и магазинах. Судом было акцентировано, что способом совершения хищения являлся обман уполномоченных сотрудников торговых организаций, который заключался в умалчивании о незаконном владении банковской картой.

Мошенники, как и информационные технологии, не стоят на месте, и постоянно прогрессируют, а именно они становятся все более изощренными, а жертв подобного вида преступлений становится все больше [3].

В последнее время популярным стало совершение дистанционного мошенничества с использованием платежных средств. Способами его совершения являются следующие [4]:

1. Вишинг. Название данного способа образовано от английского слова «vish», которое в переводе на русский язык означает «обещать, желать». Суть данного способа заключается в том, что мошенник отправляет звонок потенциальному потерпевшему от мошеннических действий с сообщением о том, что неустановленными лицами предпринималась попытка снять принадлежащие ему денежные средства с принадлежащего ему банковского счета. Для предотвращения дальнейших попыток хищения неустановленными лицами денежных средств потенциальному потерпевшему предлагается передать сведения о банковской карте, пинкоды, пароли некому представителю службы безопасности банка, который овладев личной информацией собственника банковской карты сможет «защитить»

находящиеся на ней денежные средства. Однако же в действительности осуществляется мошенничество самим лицом, представившимся сотрудником службы безопасности банка.

2. Фишинг. Название данного способа произошло от английского слова «fishing», которое в переводе на русский язык означает слово рыбалка. Суть данного способа состоит в том, что мошенники рассылают на электронные почты собственников банковских карт уведомления о необходимости перехода по ссылке на некий сайт, в котором необходимо ввести данные банковской карты для того, чтобы, например, узнать о нововведениях в условиях пользования банковской картой от лица банка или получить выигрыш вследствие участия в розыгрыше. Если лицо ввело свои данные, то они непосредственно оказываются в пользовании мошенников, которые с помощью них путем обмана совершают хищение денежных средств с банковской карты [5].

3. Выделяют и такой способ совершения мошенничества как фарминг. Его суть заключается в том, что собственники банковских карт при осуществлении ими ряда ранее привычных для них финансовых операций перенаправляются с помощью вредоносных программ на поддельные сайты. В данном случае возможно или непосредственное хищение денежных средств клиента банка путем их зачисления на мошеннический расчетный счет, либо получение данных о банковской карте человека.

Все вышеперечисленные способы дистанционного мошенничества с использованием банковских карт и иных платежных средств являются одними из наиболее сложных с позиции их расследования и выявления. Данный факт связан с тем, что в условиях совершения дистанционного мошенничества трудно определимо место совершения преступления, пути «вывода» похищенных денежных средств.

Во-первых, это связано с высоким профессионализмом преступников, которые имеют специальные знания в области информационных технологий. В настоящее время программистами с каждым днем разрабатывается все

больше программ, позволяющих условно менять территориальное расположение привязки какого-либо устройства к серверу. Такая технология именуется VPN – VirtualPrivateNetwork. При ее использовании следователь фактически не сможет установить точное местонахождение мошенника в момент совершения им преступления.

Во-вторых, значительная часть преступников с целью сокрытия денежных средств, добытых незаконным путем, использует для проведения финансовых операций криптовалюту. В данном случае проблема заключается в том, что со стороны законодательства режим использования криптовалюты как объекта гражданских прав вовсе не регламентирован. В случае, даже если следователем будет установлен факт финансовых операций в сфере использования электронной валюты, в качестве доказательства это принять будет невозможно, поскольку при оценке судом его допустимости более вероятно его исключение, так как государством данный вид денежных средств не признан, хоть и фактически он обладает всеми его признаками.

Безусловно, наиболее благоприятным для расследования представляется хищение денежных средств путем обмана с банковских карт, которые были похищены или другим способом незаконно присвоены. При расследовании такого «физического» мошенничества, следователем устанавливается место осуществления платы банковской картой, устанавливаются свидетели, по камерам видеонаблюдения формируется портрет преступника, которой впоследствии является «ориентиром» для проведения ряда оперативно-розыскных мероприятий.

Расследованию мошенничества с использованием банковских карт также препятствует ряд других факторов. Так, например, мошенники в редких случаях используют банковские счета или абонентские номера, которые юридически оформлены вовсе на других лиц. В связи с чем следователю трудно установить лиц, непосредственно совершивших преступление. Так, например, сим-карты мошенники приобретают не в салонах сотовой связи, а у иных лиц. Впоследствии нередкой является

ситуация, при которой регистрация абонентского номера осуществляется на организацию, которая вовсе не существует.

К сожалению, в настоящее время зачастую персональные данные граждан могут «утекать» из баз данных организаций, государственных или частных. Это связано с недостаточной защищенностью информации, нарушения правил ее обработки и хранения, вследствиекомпьютерных атак злоумышленников информация «утекает». Впоследствии она используется в преступных целях.

Используя определенные схемы, мошенники получают доступ к персональным данным и похищают чужие деньги. Тот факт, что телефоны стали неотъемлемой частью жизни современного общества, играет мошенникам на руку. Необходимы адекватные данной угрозе меры противодействия со стороны правоохранительных органов [6]. Для предупреждения совершения мошенничества с использованием банковских карт необходимо разрабатывать направления пропагандистской работы в отношении граждан с целью информирования их о способах совершения мошенничества с использованием банковских карт. Кроме того, на законодательном уровне необходимо закрепить необходимость использования двухфакторной аутентификации при использовании банковских карт и осуществления финансовых операций посредством их использования. Перспективным также виделось бы совершенствование взаимодействий правоохранительных органов и банковских организаций на предмет более быстрого срока исполнения запросов, предоставления иной информации о «подозрительных» движениях денежных средств по определенным банковским счетам.

Список литературы:

1. Статистика национальной платежной системы. Режим доступа – URL: https://cbr.ru/statistics/nps/psrf/

2. Приговор Советского районного суда г. Омска (Омская область) № 1-302/2020 от 29 июля 2020 г. по делу № 1-302/2020 // Режим доступа – URL: https://sudact.ru/regular/doc

3. Репухова В.Д., Влезько Д.А. Криминалистическое обеспечение расследования мошенничеств, совершенных в сети Интернет // Следственная деятельность: проблемы, их решение, перспективы развития: Материалы VI Всероссийской молодежной научно-практической конференции – Москва: Московская академия Следственного комитета Российской Федерации, 2022. – С. 329-335.

4. Козодаева О.Н., Обыденнова А.С. Способы совершения мошенничества с использованием банковских карт // Ученые записки Тамбовского отделения РоСМУ. 2019. №13.С. 65.

5. Козулина Т.И. Мошенничество с банковскими картами и методы борьбы с ним // Экономика и управление в XXI веке: тенденции развития, 2016. № 29. С. 149-153.

6. Влезько Д.А. О методах преодоления противодействия расследованию // Современные проблемы отечественной криминалистики и перспективы ее развития: Сборник научных статей по материалам Всероссийской научно-практической конференции (с международным участием), посвященной 20-летию кафедры криминалистики / Отв. ред. Г.М. Меретуков. Краснодар: Кубанский государственный аграрный университет имени И.Т. Трубилина, 2019. С. 232-238.