Научная статья
УДК 343.32+343.34
doi 10.46741/2713-2811.2024.27.3.012

Квалификация мошенничества с использованием электронного средства платежа и его отграничение от смежных составов преступлений

ВЛАДИМИР ПАВЛОВИЧ ЛЕЩЕНКО

Краснодарский университет МВД России, Краснодар, Россия, Vladimirleschenko@mail.ru

Аннотация. В статье исследуются проблемы обеспечения точной квалификации мошенничества, совершенного с использованием электронного средства платежа, в контексте реализации принципа справедливости, дифференциации уголовной ответственности и индивидуализации наказания. Выделяются ключевые особенности преодоления конкуренции между смежными составами преступлений, предметом которых являются электронные денежные средства.

Ключевые слова: хищение чужого имущества; уголовная ответственность; состав преступления; объективные признаки; банковская карта; мошенничество; платежная система; имущественный ущерб; преступление; электронное платежное средство.

5.1.4. Уголовно-правовые науки.

Для цитирования: Лещенко В. П. Квалификация мошенничества с использованием электронного средства платежа и его отграничение от смежных составов преступлений // Ius publicum et privatum: сетевой научно-практический журнал частного и публичного права. 2024. № 3 (27). С. 88–94. doi 10.46741/2713-2811.2024.27.3.012.

Original article

Qualification of Electronic Payment Fraud and Its Separation from Related Crimes

VLADIMIR P. LESHCHENKO

Krasnodar University of the Ministry of Internal Affairs of the Russian Federation, Krasnodar, Russia, Vladimirleschenko@mail.ru

Abstract. The article considers problems of ensuring the accurate qualification of fraud committed using an electronic means of payment in the context of the implementation of the principle of fairness, differentiation of criminal liability and individualization of punishment. The specifics of overcoming competition between related crimes, the subject of which is electronic money, is highlighted.

Keywords: theft of other people's property; criminal liability; composition of the crime; objective evidence; bank card; fraud; payment system; property damage; crime; electronic means of payment.

5.1.4. Criminal law sciences.

For citation: Leshchenko V.P Qualification of electronic payment fraud and its separation from related crimes. *Ius publicum et privatum: online scientific and practical journal of private and public law*, 2024, no. 3 (27), pp. 88–94. doi 10.46741/2713-2811.2024.27.3.012.

Современное общество стремительно развивается благодаря применению высоких технологий и инновационных подходов. Научно-технический прогресс охватывает все отрасли человеческой деятельности, включая товарно-денежные отношения и рыночную экономику. Сегодня депозитные и кредитные банковские карты, мобильные приложения и бесконтактные платежные системы являются основными способами оплаты сделок.

Эти изменения приводят к тому, что преступники все чаще направляют свои усилия на сектор экономики, внедряя различные способы хищения с банковских счетов и используя разнообразные преступные схемы. Государство принимает законодательные меры для предотвращения таких деструктивных действий, улучшая нормативно-правовую базу и ужесточая ответственность за экономические преступления.

В то же время параллельно осуществляется частичная либерализация уголовного наказания за отдельные виды экономических преступлений. В связи с этим полагаем, что необходимо установить равновесие между предотвращением противоправных деяний и защитой прав граждан в условиях стремительно развивающегося технологического прогресса [1].

Реализация принципа справедливости обеспечивается средствами дифференциации и индивидуализации уголовной ответственности, в том числе путем точного установления признаков состава преступления в процессе квалификации.

Одной из наиболее распространенных задач при квалификации мошенничества с использованием электронных средств платежа является уточнение критериев, отличающих его от других подобных преступлений. К таким преступлениям относятся «обычное» мошенничество (ст. 159 УК РФ), мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), кража с банковского счета и хищение электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ).

В качестве примера можно привести приговор Куйбышевского районного суда г. Омска [2]. По данным дела, работник банка С., занимавший должность сервис-менеджера в одном из отделений в Омске, обслуживал клиентку Т. Е. И., которая обратилась к нему для перевода 19 861,04 руб. с ее расчетного счета на связанный с ее картой счет. В этот момент у него возник умысел к уклонению денег гражданки Т. Е. И. Он воспользовался своим положением, чтобы сделать перевод 10 430,51 руб. со счета потерпевшей на свой счет и просил ее подтвердить операцию, используя ее карту и вводя ПИН-код. Таким образом он похитил 10 430,51 руб. и совершил еще один перевод на сумму 9 430,53 руб. для скрытия своих действий. Изначально содеянное было квалифицировано как мошенничество в сфере компьютерной информации, совершенное с использованием служебного положения.

Обстоятельства дела, представленные в приговоре, позволяют усомниться в объективности принятого судом решения. Полагаем, что содеянное образует признаки хищения

путем злоупотребления доверием, поскольку работник банка С. обманул клиентку относительно намерений и отвлек ее во время операции. Следовательно, обвиняемый совершил мошенничество. Мошенничество в области компьютерной информации обычно подразумевает изменение данных, однако в данном случае обвиняемый осуществил мошеннический перевод средств. Таким образом, в действиях виновного усматриваются признаки мошенничества, совершенного с использованием электронных средств платежа, сопряженного со злоупотреблением служебным положением (ч. 3 ст. 159[3] УК РФ).

Статистические данные, отражающие практику применения норм об ответственности за мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), позволяют говорить о ее незначительной распространенности. Так, за период с 2019 по 2023 гг. по ст. 159.6 УК РФ было осуждено 526 чел., что составляет в среднем около 130 чел. в год. Также стоит отметить, что после внесения изменений в ст. 159.3 УК РФ количество приговоров по делам о мошенничестве в сфере компьютерной информации начало снижаться [3].

Исходя из вышесказанного и учитывая тенденцию к стиранию границ между мошенничеством и мошенничеством в области компьютерной информации, некоторые исследователи предлагают объединить данные нормы. Представляется, что такой подход логичен, требует дальнейшего изучения и может стать предметом научных исследований в области борьбы с киберпреступностью.

При установлении различий между мошенничеством и кражей важно отметить, что среди специалистов нет единого мнения относительно того, как следует толковать ситуации, когда украденная или поддельная карта впоследствии используется для вывода денег через банкомат с использованием программно-технического комплекса [4]. Необходимо подчеркнуть, что в данном контексте жертвами могут стать лица, не имеющие отношения к банковской сфере. Согласно теории уголовного права, не каждое использование украденных или поддельных средств для завладения имуществом квалифицируется как мошенничество, если при этом отсутствует контакт с работниками финансовых учреждений или других специализированных организаций [5].

Практика правоприменения в полной мере отражает рассмотренную теорию.

Существует множество случаев квалификации преступлений, связанных с хищением средств через электронные платежные системы. Одним из таких может служить судебное решение по квалификации действий гражданки С., похитившей банковскую карту потерпевшего, будучи осведомленной о ПИН-коде, обналичившей 33 тыс. руб. и истратившей банковскую комиссию в сумме 345 руб. В результате чего потерпевшему был причинен значительный ущерб, а действия виновной квалифицированы по п. «г» ч. 3 ст. 158 УК РФ как тайное хищение электронных денежных средств с банковского счета [6].

Это лишь один из множества примеров правоприменения, однако далеко не единственный. Другим примером квалификации рассматриваемых преступлений являются ситуации, когда преступник осуществляет финансово-расчетные операции посредством специализированных программных систем или обналичивание денежных средств через аппаратно-программные комплексы. Показательным является приговор по уголовному делу в отношении гражданки В., действия которой были квалифицированы по ч. 2 ст. 159 УК РФ. Согласно материалам уголовного дела, гражданка похитила банковскую карту и передала ее третьему лицу, введя в заблуждение последнего, относительно имеющихся у нее прав на законное использование данной карты [7]. После того как третье лицо произвело обналичивание денежных средств в сумме 149 тыс. руб., введя ПИН-код, указанный гражданкой В., ей были переданы обналиченные деньги. В представленном примере об-

ман был использован для введения в заблуждение не потерпевшего, а третьего лица, что обеспечило сокрытие личности виновного, поэтому действия не были квалифицированы как мошенничество.

В мае 2017 г. Верховный Суд Российской Федерации принял важное постановление, согласно которому хищение денежных средств с использованием чужих электронных платежных средств через банкомат квалифицируется как кража [8]. В то же время суд указал, что при мошенничестве с использованием платежных средств обман должен быть направлен на официального представителя торговой, кредитной или иной организации. Однако в июне 2021 г. эти положения были исключены из постановления Пленума Верховного Суда Российской Федерации, что вызвало множество вопросов о том, какие действия теперь следует считать мошенничеством с использованием электронных платежных средств.

Изначальная редакция закона вызвала серьезные обсуждения среди теоретиков. Так, О. В. Ермакова указывала, что уточнение объекта обмана в предыдущей норме ограничивало круг лиц, подпадающих под данное преступление, исключая квалификацию действий злоумышленников в случаях, когда их целью не были уполномоченные специалисты указанных структур [9]. Мы полагаем, что изменения в ст. 159 УК РФ, внесенные в апреле 2018 г., которые исключили упоминание обмана уполномоченных работников, значительно расширили интерпретацию этой нормы. Также считаем, что квалификацию действий как кражи следует применять и в ситуациях, когда хищение денег посредством чужого электронного платежного средства происходит при оплате товаров на кассе самообслуживания без участия уполномоченного работника. Важно уделить внимание выявлению всех обстоятельств преступления при его квалификации в нынешних условиях.

Представленные выше примеры судебной и следственной практики свидетельствуют о различных подходах к уголовно-правовой оценке действий при краже денежных средств со счетов жертв с использованием программно-технических комплексов для автоматизированной выдачи наличности. Эти различия обусловлены как объективными причинами, такими как недостаточная законодательная регламентация, так и субъективными факторами, связанными с субъективным усмотрением правоприменителей [10]. Также вызывает споры вопрос о квалификации действий преступника, если тот использует украденную банковскую карту сотрудником для бесконтактной оплаты в торговых точках без необходимости ввода ПИН-кода на небольшие суммы или с использованием незащищенного электронного средства платежа. Некоторые эксперты считают, что в данном случае отсутствует элемент мошенничества, и, следовательно, подобные действия не могут быть квалифицированы как преступление. Сотрудник, ответственный за проведение операции, не осознает незаконности использования средств и не располагает информацией о настоящем владельце денежных активов [11].

Противоположная точка зрения основывается на признании пассивным обманом действий, состоящих в сокрытии виновным факта неправомерного использования электронного платежного средства в целях хищения денежных средств со счета потерпевшего. Данная позиция основана на том, что использование электронного платежного средства дает основание полагать лицу, осуществляющему финансово-расчетную операцию, в легитимности совершаемых действий [12].

Не менее значимой проблемой в рассматриваемом вопросе является определение квалификации действий лица, использующего одно электронное средство оплаты различными способами при совершении нескольких действий по хищению денег. Это касается сложных операций, требующих высокой квалификации со стороны правоохранительных

органов и судей. Например, мошенник может задействовать одну платежную карту для онлайн-банкинга и терминалов оплаты, проводя безналичные транзакции в магазинах и осуществляя переводы денежных средств на счета других лиц используя специализированное программное обеспечение. В данных действиях усматриваются признаки совокупности тайного хищения чужого имущества и мошенничества с использованием электронного средства платежа, объединенных единым преступным умыслом. Хотя с правовой точки зрения эти действия различаются, их общий умысел усложняет юридическую квалификацию.

Кроме того, в судебно-следственной практике встречаются случаи, связанные с совершением сложных многоуровневых преступлений, в которых активно применяются различные информационно-коммуникационные технологии и средства обработки компьютерных данных. Одна из распространенных схем включает разработку и распространение вирусов и вредоносного программного обеспечения в Интернете с целью получения доступа к личной информации пользователей. Затем эта информация используется для незаконных онлайн-транзакций или создания поддельных электронных платежных средств [13].

Эти действия должны быть квалифицированы как совокупность преступлений, однако правоохранительные органы сталкиваются с трудностями в разграничении действий по различным составам и правильной квалификации. Это связано с отсутствием опыта применения законов, разногласиями в подходах и недостаточной законодательной регламентацией.

В правоохранительной и судебной практике появилась новая проблема, связанная с мошенничеством, когда злоумышленники не стремятся напрямую завладеть деньгами, а пытаются выведать конфиденциальную информацию, такую как CVV-код, ПИН-код, пароль от мобильного банковского приложения и другие личные данные. Эти сведения открывают преступникам доступ к финансовым активам жертвы.

Обман при совершении мошенничества не служит средством для доступа к имуществу, а является способом завладения чужими средствами. Получение доступа к коду путем обмана специалиста следует рассматривать как подготовку к преступлению, а последующие действия подпадают под состав тайного хищения или мошенничества. На сегодняшний день разные правоприменители имеют разное мнение по этому вопросу.

Анализ законодательства и судебной практики показывает, что, несмотря на оптимизацию нормативной базы и разъяснения Верховного Суда Российской Федерации, возникают проблемы с квалификацией мошенничества с использованием электронных средств платежа.

В заключение можно сделать ряд выводов и предложений:

1. Оплата товаров и услуг через автоматизированную кассу без участия сотрудника должна квалифицироваться как тайное хищение с банковского счета.

2. При квалификации хищения с использованием электронных платежей необходимо учитывать все обстоятельства, включая действия, устраняющие сомнения у специалиста о правомерности использования платежа.

3. Хищения с использованием разных платежных средств должны квалифицироваться как совокупность преступлений.

4. Обман уполномоченного лица для получения информации по электронному платежу может быть квалифицирован как приготовление к краже или мошенничеству в зависимости от дальнейших действий.

5. В случаях конкуренции между составами мошенничества, указанными в ст. 159.2 и 159.3 УК РФ, следует учитывать специфику общественных отношений. Действия, не угро-

жающие отношениям собственности, должны квалифицироваться как мошенничество при получении выплат (ст. 159.2 УК РФ).

СПИСОК ИСТОЧНИКОВ

1. Ашмика А. Киберпреступления, связанные с электронными картами, и банковское мошенничество // Право и цифровая экономика. 2023. № 1 (19). С. 60–71.
2. Приговор Куйбышевского районного суда г. Омска от 11 июня 2019 г. по делу № 1-220/2019. URL: https://sudact.ru/regular/doc/BmiJ3iI64vHK/ (дата обращения: 13.11.2022).
3. Отчет о числе осужденных по всем составам преступлений Уголовного кодекса Российской Федерации и иных лиц, в отношении которых вынесены судебные акты по уголовным делам за 2023 год. URL: http://www.cdep.ru/userimages/sudebnaya_statistika/2023/k3-svod_vse_sudy-2023.xls (дата обращения: 26.02.2024).
4. Намысов Е. Д. Мошенничество в цифровую эпоху в связи с общественными изменениями // Криминологический журнал. 2023. № 3. С. 148–154.
5. Николаев Б. В., Яшина Д. Д. Мошенничество и смежные виды преступлений: проблемные вопросы разграничения // Вестник Пензенского государственного университета. 2023. № 4 (44). С. 104–108.
6. Приговор Старооскольского городского суда Белгородской области от 22 сентября 2020 г. по делу № 1-360/2020. URL: https://sudact.ru/regular/doc/OiC49lNmq9W8/ (дата обращения: 16.03.2023).
7. Приговор Кировского районного суда г. Томска от 9 марта 2016 г. по делу № 1-50/2016. URL: https://sudact.ru/regular/court/reshenya-kirovskii-raionnyi-sud-g-tomska-tomskaia-oblast/?ysclid=lvqgf8zzlw269590183 (дата обращения: 16.03.2023).
8. О судебной практике по делам о краже, грабеже и разбое : постановление Пленума Верховного Суда Российской Федерации от 27.12.2002 № 29 (ред. от 16.05.2017 № 17) // Бюллетень Верховного Суда Российской Федерации. 2003. № 2.
10. Царегородцева Р. Е. Мошенничество с использованием информационно-телекоммуникационных технологий // Вестник науки. 2023. Т. 4, № 11 (68). С. 274–279.
11. Чередниченко Е. Е. Дистанционное мошенничество: проблемы профилактики, расследования и правоприменения // Проблемы экономики и юридической практики. 2023. Т. 19, № 1. С. 211–214.
12. Базикян Н. Г. Мошенничество с использованием электронных средств платежа: особенности признаков состава преступления и вопросы квалификации // Академический научно-правовой вестник адвоката А. Н. Чашина. 2023. № 3. С. 24–29.
13. Тимиралиева С. Р. Дефинитивный набор правовой категории «мошенничество с использованием электронных средств платежа» // Система научных ценностей российского общества: междисциплинарные исследования : сб. ст. всерос. науч.-практ. конф. с междунар. участием. Таганрог, 13 января 2024 года. Уфа, 2024. С. 106–108.

REFERENCES

1. Ashmika A. Cybercrimes related to electronic cards and bank fraud. *Pravo i tsifrovaya ekonomika = Law and Digital Economy*, 2023, no. 1 (19), pp. 60–71. (In Russ.).
2. *Prigovor Kuibyshevskogo raionnogo suda g. Omska ot 11 iyunya 2019 g. po delu No. 1-220/2019* [Verdict of the Kuibyshevsky District Court of Omsk of June 11, 2019 in case No. 1-220/2019]. Available at: https://sudact.ru/regular/doc/BmiJ3iI64vHK/ (accessed November 13, 2022).
3. *Otchet o chisle osuzhdennykh po vsem sostavam prestuplenii Ugolovnogo kodeksa Rossiiskoi Federatsii i inykh lits, v otnoshenii kotorykh vyneseny sudebnye akty po ugolovnym delam za 2023 god* [Report on the number of convicts for all types of crimes of the Criminal Code of the Russian Federation and other persons against whom judicial acts on criminal

cases were issued for 2023]. Available at: http://www.cdep.ru/userimages/sudebnaya_statistika/2023/k3-svod_vse_sudy-2023.xls (accessed February 26, 2024).
4. Namysov E.D. Fraud in the digital age in relation to societal change. *Kriminologicheskii zhurnal = Criminological Journal*, 2023, no. 3, pp. 148–154. (In Russ.).
5. Nikolaev B.V., Yashina D.D. Fraud and related types of crimes: problematic issues of differentiation. *Vestnik Penzenskogo gosudarstvennogo universiteta = Bulletin of Penza State University*, 2023, no. 4 (44), pp. 104–108. (In Russ.).
6. *Prigovor Starooskol'skogo gorodskogo suda Belgorodskoi oblasti ot 22 sentyabrya 2020 g. po delu No. 1-360/2020* [Verdict of the Staryi Oskol City Court of the Belgorod Oblast of September 22, 2020 in case No. 1-360/2020]. Available at: https://sudact.ru/regular/doc/OiC49lNmq9W8/ (accessed March 16, 2023).
7. *Prigovor Kirovskogo raionnogo suda g. Tomska ot 9 marta 2016 g. po delu No. 1-50/2016* [Verdict of the Kirovsky District Court of Tomsk of March 9, 2016 in case No. 1-50/2016]. Available at: https://sudact.ru/regular/court/reshenya-kirovskii-raionnyi-sud-g-tomska-tomskaia-oblast/?ysclid=lvqgf8zzlw269590183 (accessed March 16, 2023).
8. On judicial practice in cases of theft, robbery and robbery: Resolution of the Plenum of the Supreme Court of the Russian Federation of December 27, 2002 No. 29 (as amended of May 16, 2017 No. 17). In: *Byulleten' Verkhovnogo Suda Rossiiskoi Federatsii* [Bulletin of the Supreme Court of the Russian Federation]. 2003. No. 2. (In Russ.).
10. Tsaregorodtseva R.E. Fraud using information technologies. *Vestnik nauki = Scientific Bulletin*, 2023, vol. 4, no. 11 (68), pp. 274–279. (In Russ.).
11. Cherednichenko E.E. Remote fraud: problems of prevention, investigation and law enforcement. *Problemy ekonomiki i yuridicheskoi praktiki = Economic Problems and Legal Practice*, 2023, vol. 19, no. 1, pp. 211–214. (In Russ.).
12. Bazikyan N.G. Fraud using electronic means of payment: features of the elements of a crime and qualification issues. *Akademicheskii nauchno-pravovoi vestnik advokata A. N. Chashina = Academic Scientific and Legal Bulletin of the Lawyer A.N. Chashin*, 2023, no. 3, pp. 24–29. (In Russ.).
13. Timiralieva S.R. A definitive set of the legal category "fraud using electronic means of payment". In: *Sistema nauchnykh tsennostei rossiiskogo obshchestva: mezhdistsiplinarnye issledovaniya: sb. st. vseros. nauch.-prakt. konf. s mezhdunar. uchastiem. Taganrog, 13 yanvarya 2024 goda* [System of scientific values of the Russian society: interdisciplinary research: collection of articles of the All-Russian scientific and practical conference with international participation. Taganrog, January 13, 2024]. Ufa, 2024. Pp. 106–108. (In Russ.).

СВЕДЕНИЯ ОБ АВТОРЕ / INFORMATION ABOUT THE AUTHOR

ЛЕЩЕНКО ВЛАДИМИР ПАВЛОВИЧ – преподаватель кафедры социально-гуманитарных дисциплин Краснодарского университета МВД России, Краснодар, Россия, Vladimirleschenko@mail.ru

VLADIMIR P. LESHCHENKO – Lecturer at the Department of Social and Humanitarian Disciplines of the Krasnodar University of the Ministry of Internal Affairs of the Russian Federation, Krasnodar, Russia, Vladimirleschenko@mail.ru

Статья поступила 30.07.2024