К ВОПРОСАМ О ПРОТИВОДЕЙСТВИИ МОШЕННИЧЕСТВУ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА

TO QUESTIONS ABOUT COMBATING FRAUD USING ELECTRONIC MEANS OF PAYMENT

S. Kropachev

Summary. The article discusses the problematic aspects of the criminal law composition of fraud using electronic means of payment. An analysis of various points of view on the existing problems of differentiating related fraud structures allows us to conclude that at the moment the state of legal regulation of protection against fraud using electronic means of payment has a number of shortcomings and requires further improvement, as well as insufficient attention is paid to strengthening organizational and economic measures character for the prevention of this type of crime. The author of the article makes an attempt to systematize the existing points of view on issues of deficiencies, legislation gaps that establish liability for fraud using electronic means of payment, and also makes suggestions for further improvement of legislation in this area.

Keywords: Fraud, common and special norms, crime, information technology, electronic means of payment, article 159.3.

Кропачев Сергей Юрьевич
Адъюнкт, Нижегородская академия МВД России
skropach@mail.ru

Аннотация. В статье рассматриваются проблемные аспекты уголовно-правового состава мошенничества с использованием электронных средств платежа. Анализ различных точек зрения по существующим проблемам разграничения смежных составов мошенничества позволяют сделать вывод о том, что на данный момент состояние правового регулирования защиты от мошенничества с использованием электронных средств платежа имеет ряд недостатков и требует дальнейшего совершенствования, а также недостаточно внимания уделяется усилению мер организационного и экономического характера по профилактике данного вида преступлений. Автор статьи предпринимает попытку систематизации существующих точек зрения по вопросам недостатков, пробелов законодательства, устанавливающих ответственность за мошенничество с использованием электронных средств платежа, а также вносит свои предложения по дальнейшему совершенствованию законодательства в данной области.

Ключевые слова: Мошенничество, общая и специальная нормы, преступление, информационные технологии, электронное средство платежа, статья 159.3.

В настоящее время рынок банковских услуг, на общем фоне совершенствования информационных технологий, придерживается четкой тенденции на совершенствование услуг, предоставляемых в электронном виде, и продвижение расширенного спектра возможностей удаленного доступа к расчетным счетам для совершения платежей и переводов клиентам кредитных организаций. «Так, количество транзакций, совершаемых клиентами дистанционно через удаленные каналы обслуживания, у ведущих банков страны и платежных систем ежегодно увеличивается и в настоящее время достигает более 95% от числа всех операций» [1].

Банком России в течение нескольких лет был осуществлен ряд мероприятий по измерению показателей финансовой доступности, в результате которых статистические данные использования клиентами возможностей удаленного доступа к услугам, предоставляемых кредитными организациями, показали устойчивый рост, с 45.1% в 2017 году до 55,6% в 2019 году. Необходимо отметить, что при общем прогрессе использования в финансовой сфере безналичных расчетов, представители уголовно-правовой науки не видели необходимости во внедрении отдельного состава мошенничества. Тем не менее, законодатель посчитал нужным применить в диспозиции статьи 159.3 УК РФ, вместо платежной карты, значительно более масштабное понятие — электронное средство платежа.

Полагаем, что намерение урегулировать проблему мошенничества в сфере платежей, осуществляемых с использованием электронных средств, одними только уголовно-правовыми средствами не привело к ожидаемому результату вследствие недостаточно детальной проработки вопроса.

Электронные средства платежа, в качестве средства совершения преступления, были введены в диспозицию статью 159.3 УК РФ Федеральным законом «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» [2], что и стало ключевым изменением данной статьи. Таким образом, если исходить из общего смысла мошенничества, то очевидно законодатель имел в ввиду, что субъект деяния, путем использования электронного средства платежа, руководствуясь корыстным мотивом, должен обмануть конкретное лицо. Собственно, сама необходимость введения такого термина, как "электронные средства платежа" была в первую очередь связана с тем, что Уголовный кодекс РФ и Федеральный закон «О национальной платежной системе» [3] не имели единых стандартизованных подходов относительно терминологии.

Понятие «электронное средство платежа» закрепляется пунктом 19 статьи 3 Федерального закона «О национальной платежной системе» [3], где под электронным средством платежа понимается средство и (или) способ, посредством которого клиент кредитной организации может составлять, удостоверять и передавать распоряжения для перевода денежных средств, используя действующие виды безналичных расчетов с использованием информационных-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств.

Несомненно, что увеличивая круг средств совершения мошенничества, законодатель принял во внимание общий прогресс развития информационных технологий в финансовой сфере, позволяющий проводить дистанционные операции посредством все большего количества разнообразных типов программно-аппаратных устройств и сформировавшуюся вследствие этого направленность на переход в безналичный денежный оборот для кредитных и платежных операций. Так, например, пунктом 1.1 Положения о правилах осуществления перевода денежных средств[4], утвержденного Банком России, закрепляется проведение кредитной организацией перевода денежных средств по банковским счетам, а также и без открытия таковых, в рамках реализации форм безналичных расчетов, где использование электронных средств платежа определяется договором перевода денежных средств между оператором и его клиентом, а их использование при обычном переводе электронных денег служит необходимым условием. Во многом благодаря именно развитию информационных технологий и получили такое распространение электронные средства платежа.

В соответствии с п. 1 ст. 9 ФЗ «О национальной платежной системе» между кредитной организацией и клиентом, а также между кредитными организациями, при осуществлении банковских операций заключается договор об использовании электронных средств платежа и общепринятым основанием для заключения подобного договора является наличие договорных отношений между банком и клиентом. Немного отличается ситуация с переводом электронных денежных средств, где как такового договора об использовании электронного средства платежа не предусмотрено, а условие на его использование прописывается в договоре перевода электронных денежных средств, который может заключаться между клиентом и кредитной организацией и без наличия между ними отношений по переводу денежных средств (например, при отсутствии открытого расчетного счета клиента).

Таким образом, по своей сути электронные средства платежа не являются расчетным документом, так как применяются в операциях по переводу, как электронных и безналичных финансовых средств, так и для зачисления и выдачи наличных денег.

Выделим основные виды электронных средств платежа:

1. Интернет-банкинг (онлайн-банкинг), представляющий собой способ удаленного обслуживания кредитной организацией клиентов, с предоставлением им возможности дистанционного управления своими расчетными счетами посредством информационно-телекоммуникационной сети «Интернет»;
2. Платежные карты, используемые для осуществления операций посредством банкоматов, электронных терминалов;
3. Операции CNP (card not present), то есть действия только по реквизитам карты, без ее фактического использования, через информационно-телекоммуникационную сеть «Интернет»;
4. Электронные кошельки («QIWI Wallet», «Яндекс. Деньги» и др.) — электронные средства платежа, предоставляющие возможность осуществления безналичной оплаты товаров и услуг, посредством предварительно внесенных денежных средств без открытия счета;
5. Электронные программно-технические устройства, специально разработанные для осуществления удаленного перевода денежных средств (например, POS-терминал).

Остановимся подробнее на тех моментах, которые на наш взгляд нуждаются в корректировке.

При более тщательном рассмотрении основных видов электронных средств платежа, с учетом специфики их использования, становится очевидным, что совершение мошенничества посредством поддельного или принадлежащего иному лицу электронного средства платежа, возможно совершить только посредством платежных карт. На это указывал законодатель в предыдущей редакции ч. 1 ст. 159.3 УК РФ, используя такую формулировку, как "…с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем обмана уполномоченного работника кредитной, торговой или иной организации…".

Между тем в ФЗ «О национальной платежной системе» [3] идет речь только о легальных электронных средствах платежа, применяемых на основании заключенных договоров, и в настоящей момент в диспозиции ст. 159.3 УК РФ не указана возможность того, что электронное средство платежа может быть поддельным или принадлежать иному лицу. На наш взгляд это может не-

гативно повлиять на практическое применение данной статьи, потому что в УК РФ ответственность за мошенничество в сфере компьютерной информации установлена ст. 159.6 УК РФ, в соответствии с которой способами совершения этого вида преступления являются введение, уничтожение, блокирование, изменение компьютерной информации, а также другое воздействие на процессы работы средств сбора, обработки, хранения и использования компьютерной информации или информационно-телекоммуникационных сетей.

В связи с этим последовало обоснованное разъяснение указанных положений ст. 159.6 УК РФ со стороны Пленума Верховного суда РФ[5] об ограничении толкования способов совершения указанного мошенничества, определив в качестве такового только целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники или на информационно-телекоммуникационные сети, что в свою очередь не может быть совершено путем применения электронного средства платежа.

Необходимо отметить, что без данного разъяснения в большинстве случаев разграничение преступлений, предусмотренных п. «г» ч. 3 ст. 158, ст. 159.3 и ст. 159.6 УК РФ, представлялось бы крайне затруднительным.

В тех случаях, когда владелец лично, но в результате обмана или злоупотребления доверием со стороны злоумышленника, передает последнему конфиденциальную информацию (например, персональные данные, информацию о карте, пароли), открывающую доступ к электронному средству платежа, после чего происходит хищение безналичных денежных средств, то нам представляется, что действия преступника подлежат квалификации по ст. 158 УК РФ.

Аналогичным образом, нам близка позиция ряда ученых, которые считают, что не является мошенничеством хищение денежных средств с расчетных счетов кредитной организации, посредством похищенной или поддельной платежной карты, путем снятия наличных денежных средств через банкомат, в том числе используя скимминг[6, с. 57]. На это указывает и разъяснение Пленума Верховного суда РФ[5] о том, что необходимо квалифицировать хищение денежных средств с расчетных счетов кредитных организаций, как мошенничество с использованием электронного средства платежа только в тех случаях, когда хищение сопровождалось обманом конкретного физического лица о том, что электронные средство платежа принадлежит злоумышленнику на легальном основании.

Неразрешенным остается вопрос об объекте обмана, является ли им только собственник или иной законный владелец, или это может быть более широкий круг лиц, подвергнувшихся обману.

По данной позиции мнения ученых неоднозначны, так Л. В. Боровых, Е. А. Корепанова, считают, что обман сотрудника кредитной организации, который совершает субъект преступления с целью получения денежных средств, служит только средством облегчения доступа к имуществу[7, с. 100].

Необходимо понимать, что общепринятое понятие мошенничества основывается на том, что обман направлен в адрес собственника или иного законного владельца имущества, иначе отсутствует добровольный мотив сделки, а это именно тот признак, который характерен только для мошенничества. Например, Н. А. Лопашенко считает, что при совершении мошенничества сам факт получения имущества непосредственно от потерпевшего происходит внешне добровольно, но вследствие информационного воздействия на волю последнего происходит искажение реальных обстоятельств и он желает передать виновному имущество[8, с.275]. Подобной точки зрения придерживаются и другие ученые, например Е. Е. Черных[9, с. 372]. Для примера, в случае, когда преступник заранее зная об отсутствии денежных средств на счете, в присутствии потерпевшего посредством онлайн-банкинга направляет заявку в кредитную организацию о переводе денежных средств на счет потерпевшего, поясняя, что денежные средства зачислят на счет в течение 3 рабочих дней, как установлено п. 5 ст. 5 Федерального закона «О национальной платежной системе» [3], тем самым вводя потерпевшего в заблуждение относительно факта окончательного расчета и совершает хищение товара.

Тем не менее, Пленум Верховного Суда РФ отмечает[5], что объектом преступления является либо владелец имущества, либо другое лицо, а это в свою очередь указывает на то, что потерпевшими могут быть и третьи лица, в качестве таковых в предыдущей редакции ст. 159.3 УК РФ были указаны работники торговой, кредитной или иной организации.

Изучив данную проблему, мы считаем, что обман сотрудника кредитной или другой организации при осуществлении операций по поддельной или чужой платежной карте служит средством облегчения доступа к имуществу, а не способом изъятия. Учитывая это, необходимо поддержать позицию ученых, считающих, что совершение мошенничества, предусмотренного ст. 159.3 УК РФ, в классическом понимании таковым не является и подобные преступления правильнее квалифицировать как кражу[10, с. 76].

При анализе рассматриваемого вопроса становится очевидным, что законодатель при введении данной

нормы не установил четко определенные границы преступления, в котором в качестве средства совершения выступает электронное средство платежа.

Так, например, одной из проблем является конкуренция ст. 159.3 и 159.6 УК РФ в тех случаях, когда в процессе использования электронного средства платежа в присутствии сотрудника банковской, либо другой организации осуществляется ввод PIN-кода, вследствие чего происходит преобразование компьютерной информации, что позволяет, по мнению ряда ученых, считать ст. 159.3 УК РФ специальной по отношению к ст. 159.6 УК РФ[11, с. 240]. В данном случае мы считаем, что квалификация должна осуществляться по ст. 159.3 УК РФ, так как введение PIN-кода составляет лишь часть способа совершения преступления.

По нашему мнению можно дополнить ст. 159.3 УК РФ частью 2 в следующем виде «…мошенничество с использованием платежных карт с помощью электронно-вычислительных машин или других программно-аппаратных средств, либо путем разработки фиктивных программ, использования недостоверных данных, посредством нелегитимного использования данных или иного неправомерного воздействия на результат обработки данных».

Еще одной проблемой является квалификация мошенничества в зависимости от способа совершения при использовании либо подлинной (например, найденной), либо изготовлении поддельной платежной карты, либо внесении ложных данных в подлинную платежную карту[12, с. 32].

В ряде случаев хищение денежных средств банковской организации посредством карты, полученной преступником в результате обмана, или вообще произведенной на имя физического лица без его согласия, расценивается судами как мошенничество сфере кредитования, ответственность за которое устанавливается ст. 159.1 УК РФ. Но встречаются случаи, когда преступником является сотрудник банковской организации, который посредством оформления фиктивных договоров займа, без ведома граждан, завладевает кредитной картой и распоряжается ей по своему усмотрению, и суды в данном деянии усматривают и ч. 3 ст. 159 УК РФ, и мошенничество с использованием платежных карт. Таким образом, получается что, по сути, аналогичные деяния могут квалифицироваться по-разному в правоприменительной практике.

Как свидетельствует статистика Европейского союза, значительная часть, достигающая почти 60%, мошеннических переводов денежных средств производится в результате транзакций без фактического присутствия карты [13], вследствие чего возникает вопрос о квалификации таких преступлений. Пленум Верховного суда РФ полагает, что данные деяния необходимо квалифицировать как кражу[5], и это мнение нашло свое подтверждение в научной литературе. Например, И. А. Александрова считает, что хищение денежных средств с расчетного счета объекта преступления посредством несанкционированного доступа к системе дистанционного банковского обслуживания не образует состава мошенничества в силу того, что отсутствуют конкретные лица, обманутые или введенные в заблуждение злоумышленником[14]. При этом, необходимо обратить внимание на то, что мошенничество в сфере компьютерной информации квалифицируется по ст. 159.6 УК РФ и в том случае, когда отсутствует обман физического лица, а имеется, если можно так выразиться, "обман" ЭВМ.

Следующий момент, нуждающийся в корректировке, связан с разъяснением термина "использовать" применительно к электронным средствам платежа. ФЗ «О национальной платежной системе» предусмотрено использование электронных средств платежа только для составления, удостоверения и передачи распоряжения о переводе безналичных и электронных денежных средств. Таким образом, либо хищение иного имущества и приобретение права на имущество данной редакцией статьи не охватывается, либо под использованием понимать другое применение, с умыслом на совершение преступления, чтобы охватить данной нормой эти деяния.

Как показывает статистика, каждый год с банковских счетов россиян похищают около 1 млрд. рублей. Объем операций по расчетным счетам банковских карт, оценивается в 100 трлн. рублей, для сравнения бюджет России составляет 15 трлн. рублей.

Нашел свое подтверждение и рост количества несанкционированных операций с использованием платежной карты. Так, на территории России и за ее пределами объем несанкционированных операций с использованием платежных карт, выпущенных российскими кредитными организациями, в 2018 г. составил 1,384 млрд. руб. (в 2017 г.— 0,961 млрд. руб., в 2016 г.— 1,08 млрд. руб., в 2015 г.— 1,14 млрд. руб.)[15].

Осознав серьезность проблемы, помимо уголовно-правовых мер с хищениями посредством электронных средств платежа законодатель вносит изменения в ФЗ «О национальной платежной системе», одним из направлений которого, является минимизация рисков безвозвратных потерь денег потерпевшими в связи с незаконным использованием их карт в преступных целях. Например, ст. 9 вышеупомянутого закона, указывающая на необходимость возмещения банком ущерба клиенту в том случае, если перевод денежных средств произой-

дет без согласия последнего при своевременном извещении клиентом финансовой организации об утере электронного средства платежа и (или) использования последнего без согласия клиента.

Таким образом, успешно решить проблему борьбы с мошенничеством с использованием электронных средств платежа только уголовно-правовыми средствами, в том числе усилением ответственности, не представляется возможным.

По результатам рассмотрения данного вопроса можно сделать следующие выводы:

- мошенничество с использованием электронных средств платежа не соответствует пониманию мошенничества в его традиционном виде;
- в действующей редакции ч. 1 ст. 159.3 УК РФ отсутствует указание в отношении кого направлен обман, например работников кредитной, торговой или иной организации, как в предыдущей редакции данной статьи;
- налицо возникновение проблем в квалификации составов преступлений указанных в ст. 159.3 УК РФ и п. «г» ч. 3 ст. 158 УК РФ, ст. 159.1, 159.6 УК РФ, в силу того, что электронные средства платежа используются как в сфере кредитования, так и в сфере компьютерной информации;
- необходимо проводить профилактику мошенничества посредством усиления мер экономического и организационного характера, направленных на снижение рисков потери денежных средств клиентами финансовых организаций в связи с использованием электронных средств платежа, в том числе улучшением защиты средств дистанционного доступа к банковским услугам.

Из всего изложенного становится очевидным, что назрела насущность принятия ряда мер экономического, организационного и уголовно-правового характера, а также внесения необходимых изменений в действующее законодательство, что, очевидно, должно лечь в основу отдельного системного научного исследования.

ЛИТЕРАТУРА

1. Пояснительная записка «К проекту федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации (в части усиления уголовной ответственности за хищение денежных средств с банковского счета или электронных денежных средств)»: [Электронный ресурс] Автоматизированная система обеспечения законодательной деятельности. URL: http://asozd.duma.gov.ru/ (дата обращения 20.01.2020)
2. Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» от 29.11.2012 № 207-ФЗ // Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 23.01.2020).
3. Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе» // Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 23.01.2020)
4. Положение Банка России от 19.06.2012 N383-П (ред. от 11.10.2018) «О правилах осуществления перевода денежных средств» // Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 23.01.2020).
5. Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 23.01.2020).
6. Хилюта В. В. Хищение с использованием компьютерной техники или компьютерное мошенничество // Библиотека криминалиста. 2013. № 5.— С. 55–65
7. Боровых Л. В., Корепанова Е. А. Направленность обмана в составе мошенничества с использованием платежных карт // Вестник Пермского университета. 2016. Вып. 1(31).— С. 98–104
8. Лопашенко, Н. А. Посягательства на собственность — М.: Норма, Инфра-М, 2012.— 528 с.
9. Черных Е. Е. Особенности законодательного закрепления ответственности за новые виды мошенничества // Дифференциация и индивидуализация ответственности в уголовном и уголовно-исполнительном праве. Мат. межд. науч.-практ. конф. / Под редакцией В. Ф. Лапшина., 2015,— С. 367–372
10. Чесноков М. В. Обман как способ совершения мошенничества в сфере кредитования // Успехи современной науки и образования. 2016. Т. 2. № 5. С. 76–78.
11. Шебанов Д. В., Терещенко Л. С. О некоторых проблемах квалификации мошенничества в сфере компьютерной информации // Теория и практика общественного развития. 2014. № 4.— С. 240–242.
12. Яни П. С. Мошенничество: момент возникновения умысла // Законность. 2017. № 5.— С. 32–36
13. FICO: «Europe's Card Fraud Is Evolving» [Электронный ресурс] Интернет-журнал «ПЛАС» — издание, посвященное вопросам финансового обслуживания населения, банковской розницы и платежной индустрии. URL: https://www.plusworld.ru/journal/section_1586/section_187288/art187282/ (дата обращения 25.01.2020)
14. Александрова И. А. Новое уголовное законодательство о мошенничестве // Юридическая наука и практика: Вестник Нижегородской академии МВД России, 2013. № 21.— С. 54–62
15. Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России 1.09.2018–31.08.2019// [Электронный ресурс]: Официальный сайт Центрального банка РФ. URL: http://www.cbr.ru/fincert/ (дата обращения 26.01.2020).

Журнал «Современная наука: актуальные проблемы теории и практики»