Экономический факультет МГУ имени М.В. Ломоносова

ОЛИМПИАДА ПО ФИНАНСОВОЙ ГРАМОТНОСТИ

2019

Авторы:

Самус Анастасия Михайловна
anastasiyasamus@mail.ru

Головань Мария Вячеславовна
golovan.maria2015@yandex.ru

Яцкина Дарья Николаевна
dariya_yatskina@mail.ru

Лысенко Юлия Сергеевна
yuliya.lysenko.1998@mail.ru

Павлова Элла Владимировна
katu97.97@mail.ru

Преподаватель-тренер:

К.э.н., доцент Золотова Елена Алексеевна, zolotowa@mail.ru

Северо-Кавказский федеральный университет

Команда «Золотой Запас»

СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ ОКРУГ

Незаконное списание средств с банковской карты при оплате услуг через интернет

Ставрополь 2019

Оглавление

Введение

В 2018 году было выпущено более 270 млн банковских карт, то есть примерно 2,5 штук на каждого взрослого жителя России[1]. Данный факт подтверждает то, что пользование безналичными средствами приобретает интенсивный характер. Это связано с тем, что банковские карты снижают объем наличных платежей, тем самым экономят время держателей карт, т. к. у пользователей появляется возможность совершать платежи дистанционно. Однако, с другой стороны, наличие большого количества карт провоцирует рост финансового мошенничества в сети Internet, как в случае с нашим героем.

По данным МВД в январе-июле 2018 года было зарегистрировано 741 преступление по ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации» и 564 преступления по ст. 159.3 УК РФ «Мошенничество с использованием электронных средств платежа»[2]. Феномен Интернет-мошенничества в наше время приобретает широкое распространение, а главное влечет за собой сильные социальные последствия, поэтому для нас актуально изучение данного явления.

В представленном кейсе под названием «Незаконное списание средств с банковской карты при оплате услуг через интернет» рассматривается проблема незаконного списания денежных средств с банковской карты.

Цель нашей работы состоит в изучении предложенного кейса и разработке решений описанной в нем проблемы, а также в определении профилактических мер по недопущению повторения аналогичных случаев.

Для достижения поставленной цели были определены следующие задачи:

1. Изучить действующую нормативную базу РФ, в которой рассматривается списание денежных средств с банковской карты, оплата услуг через интернет и другие нормативные акты, связанные с данными ситуациями.

[1] https://www.sberbank.ru/common/img/uploaded/files/pdf/analytics/bank_trends_2018.pdf
[2] https://www.gazeta.ru/business/2018/11/15/12060103.shtml

2. Выявить интересы стейкхолдеров данного кейса, их противоречия и взаимную увязку.

3. Определить возможные направления урегулирования списания средств с банковской карты при оплате услуг через интернет, их плюсы и минусы.

4. Разработать предпочтительный вариант по списанию средств с банковской карты при оплате услуг через интернет.

В ходе написания работы применялись следующие методы исследования: анализ, синтез, индукция, дедукция, наблюдение, сравнение, группировка.

Информационную базу исследования составили законодательные и нормативные акты Российской Федерации, научные труды, статистические материалы, статьи периодических изданий, ресурсы сети Интернет.

Основная часть

Обзор действующей нормативной базы

При изучении законодательства, регулирующего правовые и организационные основы национальной платежной системы (НПС) и, в частности, 161-ФЗ «О национальной платежной системе»[3] было выявлено, что в ст. 9 «Порядок использования электронных средств платежа» данного закона имеются следующие положения:

- оператор обязуется уведомлять своих клиентов о совершении каждой электронной оплаты;

- электронное платежное устройство может быть приостановлено при соответствующем обращении от клиента;

- если средства с электронной системы были списаны без ведома клиента, то оператор обязуется возместить ущерб.

Данные положения способствуют борьбе с незаконным списанием средств, однако в них есть ряд недоработок, в связи с которыми возникают споры при решении судебных дел, связанных с проблемой незаконного списания средств с банковских карт. Одной из таких недоработок является то, что закон о НПС не ограничивает возможные способы информирования клиентов о совершенных операциях, т. е. уведомление могут приходить как в «личный кабинет», так и через SMS-сообщения или при помощи иного аналогичного Интернет-сервиса. При нерегулярном использовании «личного кабинета» или иного интернет-сервиса, в который банк отправляет уведомления, клиент может несвоевременно

[3] http://www.consultant.ru/document/cons_doc_LAW_115625/

отреагировать на незаконное списание средств с банковской карты, что препятствует эффективной борьбе с интернет-мошенничеством в данной сфере.

Кроме того, закон о НПС не определяет момент, в который уведомление об операции с использованием электронного средства платежа (ЭСП) считается полученным клиентом, что также немаловажно, т. к. клиент должен обратиться с информацией о незаконном списание средств в течение одного дня после получения уведомления[4]. Помимо этого, в 161-ФЗ нет четких указаний о том, что должно быть прописано в уведомлении, как это делается в международном законодательстве.

В частности, рассмотрим ст. 47 Нормы Директивы 2007/64/ЕС, где четко регламентировано, что после того, как сумма разовой платежной операции была снята со счета плательщика, провайдер платежных услуг плательщика должен безотлагательно предоставить ему следующую информацию в порядке, определенном ст. 41 этой Директивы:

- реквизиты, позволяющие плательщику идентифицировать каждую платежную операцию и при необходимости информацию, относящуюся к получателю средств;

- сумму платежной операции в валюте дебетования расчетного счета плательщика или в валюте, использованной в платежном поручении;

- объем любых сборов за проведение платежной операции и при необходимости их детализация или процентные выплаты плательщика;

- дату дебетования или дату получения платежного поручения[5].

Отражение всех этих данных повышает эффективность идентификации интернет-мошенников, т. к. клиент в этом случае точно знает, куда были списаны незаконным путем его средства с банковской карты, и может обратиться с заявлением на определённых лиц в правоохранительные органы.

Однако введение подобного опыта в РФ на данный момент невозможно, так как это противоречит законодательству РФ, а именно Федеральному закону от 27.07.2006 N 152-ФЗ (ред. от 31.12.2017) «О персональных данных».

Также в 161-ФЗ нет точного указания о порядке использования электронного средства платежа, банки прописывают его в договоре, и поэтому держателям карт в суде практически невозможно доказать, что порядок не был нарушен.

Рассматривая проблему незаконного списания средств, также важно обратить

[4] http://www.cbr.ru/Content/Document/File/16195/faq_9.pdf
[5] https://www.cbr.ru/PSystem/regulation_p/compare161/

внимание на Постановление Правительства РФ от 27.09.2007 № 612 (ред. от 04.10.2012)[6] «Об утверждении Правил продажи товаров дистанционным способом», которое регулирует законное совершение покупок через всемирную сеть. В данном постановлении указано, что договор считается заключенным с момента выдачи продавцом покупателю кассового или товарного чека, либо иного документа, подтверждающего оплату товара, или с момента получения продавцом сообщения о намерении покупателя приобрести товар. Следовательно, если онлайн-организация не предоставила документ, который бы подтверждал совершение покупки потребителем, то снятие денежных средств с банковской карты следует признать незаконным.

Помимо этого, согласно ст. 845 ГК РФ[7], одной из наиболее важных экономических целей договора банковского счета является сохранность денежных средств клиента, размещенных в банке. В данной статье также закреплено положение, согласно которому списание денежных средств со счета клиента допускается банком на основании распоряжения клиента. Если банки проводят идентификацию клиента без ввода PIN-кода, основываясь только на правильности введения CVV/CVC2-кода, то они нарушают правила идентификации лица, имеющего право распоряжения денежными средствами на счете и согласно п. 2 Постановления Пленума ВАС РФ от 19.04.1999 № 5[8], банк будет обязан нести ответственность за последствия исполнения поручений, выданных неуполномоченными лицами, так как возникнет состав гражданского правонарушения, необходимый для возложения на него гражданско-правовой ответственности за причиненный вред, выразившийся в неправомерном списании денежных средств со счета клиента. В таких ситуациях банки обычно ссылаются на то, что клиент нарушил порядок пользования ЭСП, однако этот довод можно считать несостоятельным, поскольку он носит гипотетический характер, а в соответствии с закрепленным в ст. 10 ГК РФ[9] принципом добросовестности, пока не доказано иное, действия клиента считаются добросовестными.

Интересы стейкхолдеров

Для того чтобы найти решение проблемы незаконного списания средств с банковской карты при оплате услуг через интернет, необходимо определить стейкхолдеров, т. е. стороны, заинтересованные в решении данной проблемы, и выявить взаимоувязку и противоречие их интересов. Такими сторонами являются сами держатели карт, банки,

[6] http://www.consultant.ru/document/cons_doc_LAW_71418/
[7] http://www.consultant.ru/document/cons_doc_LAW_9027/9e5d4849d8ca1f3cd88dff170479109e12b2f3be/
[8] http://www.consultant.ru/document/cons_doc_LAW_23458/
[9] http://www.consultant.ru/document/cons_doc_LAW_5142/62129e15ab0e6008725f43d63284aef0bb12c2cf/

интернет-магазины и регулятор. Рассмотрим подробнее интересы каждого из стейкхолдеров.

Держатели карт заинтересованы в экономии своего времени, поэтому онлайн-переводы денежных средств и интернет-покупки с использованием банковских карт становятся популярнее с каждым годом. В 2017 году у россиян на 11% по сравнению с предыдущим годом возросла доля безналичных операций в расходных операциях по картам, эта тенденция продолжалась и в 2018 году, в первом полугодии произошел рост еще на 12%[10].

Стоит также отметить, что потребители склонны покупать в сети Internet больше, чем они могут себе позволить, используя для этого банковские кредитные карты, о чем свидетельствует статистика. По данным ЦБ РФ в 2017 году по сравнению с 2016 годом почти на треть увеличилось число операций с использованием электронных технологий (до 25,4 млрд распоряжений), совершенных клиентами кредитных организаций, а объем таких операций возрос на 10,5% (до 592,6 трлн рублей), причем 20% платежей совершались с использованием мобильных устройств связи или в сети Internet[11]. Держатели карт заинтересованы в безопасной оплате товара (работ, услуг) через интернет посредством банковской карты, т. к. они не хотят рисковать своими деньгами. Помимо этого, потребителей волнует возврат средств, списанных из-за интернет-мошенников.

Также в борьбе с незаконным списанием средств с банковской карты при оплате услуг через интернет заинтересованы интернет-магазины, поскольку онлайн-платежи позволяют многократно увеличить объем продаж, сделав товар или услугу доступной в любой точке мира, а также снизить затраты на содержание офиса и сократить штат сотрудников. Эксперт по интернет исследованиям Федор Вирин во время своего выступления на РИФ 2018 с докладом «Интернет-торговля в России» отметил, что интернет-продажи за 2017 год возросли на 18%[12]. Мошенничество при онлайн-платежах ведет к утрате доверия клиентов, что влечет за собой денежные потери интернет-магазинов, поэтому они также стремятся к снижению незаконного списания средств.

Еще одной заинтересованной стороной в безопасности интернет-операций с использованием банковских карт являются банки. Они рискуют не только своими деньгами, в том случае, если им придется возвращать денежные средства, списанные незаконным путем, держателю карты, но и своей репутацией, что в свою очередь может повлечь за собой

[10] https://www.sberbank.ru/common/img/uploaded/news/2018/cash_and_cashless_payments.pdf
[11] http://www.cbr.ru/Content/Document/File/59588/results_2016-18.pdf
[12] http://www.fedorvirin.ru/conference18/

отказ потребителей от услуг данного банка и опять же финансовые потери. Банковские карты, а в особенности кредитные, дают огромные доходы банкам, это связано с тем, что, во-первых, банки получают плату за обслуживание карт с потребителей, а в случае кредитных карт еще комиссии, проценты и штрафы, которые начисляются банками за нарушение правил использования кредитных карт. Во-вторых, владельцы карт становятся автоматически клиентами банка и часто начинают пользоваться его дополнительными услугами. В-третьих, карты позволяют аккумулировать большие денежные потоки внутри банка, и наконец, банк-эквайер получает комиссию за произведенные финансовые операции. Именно поэтому с каждым годом банки внедряют все более новые, совершенные и одновременно дорогостоящие средства безопасности онлайн-платежей и защиты от мошенников.

Кроме того, в безопасной оплате услуг через интернет заинтересован регулятор в лице ЦБ, законодательного и исполнительного органа власти РФ, поскольку незаконное списание денежных средств с банковских карт препятствует развитию цифровой экономики в России, а именно создает угрозы развития малого и среднего бизнеса, подрывает доверие граждан к отечественному банковскому сектору, а также ведет к нарушению прав человека в цифровом мире. Отметим, что Правительством РФ в 2017 году была утверждена программа «Цифровая экономика Российской Федерации», которая направлена на повышение уровня цифровой экономики в России[13]. Сам регулятор также вводит изменения в законодательство для усовершенствования борьбы с мошенничеством. Так, например, в 2018 году были внесены изменения в 9 статью 161-ФЗ «О национальной платежной системе», которые усилили защиту прав держателей карт.

Таким образом, интересы всех стейкхолдеров сходятся в том, чтобы минимизировать незаконное списание денежных средств с банковских карт при онлайн-платежах, а также снизить именно свои риски при потерях от мошенников. Здесь и начинают возникать противоречия стейкхолдеров, т. к. если риски снижаются у одной стороны, то повышаются у другой. Так, например, если будут внесены изменения в ряд положений 161-ФЗ (Приложение 1), улучшится положение держателей карт в спорных моментах по мошенничеству, поскольку в суде потребители смогут апеллировать внесенными изменениями, однако это также приведет к потерям банков, которые должны будут возместить причиненный мошенниками ущерб. Если же банки решат снизить свои риски путем ужесточения проверки онлайн-платежей, то это, скорее всего, приведет к тому,

[13] http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf

что процедура оплаты станет отнимать у держателей карт больше времени. Впоследствии это может привести к тому, что снизится уровень онлайн-платежей, а, следовательно, и уровень продаж, поэтому интернет-магазины понесут финансовые потери. В связи с этим необходимо во время разработки решения проблемы незаконного списания средств обращать внимание на сопоставимость интересов стейкхолдеров, выявлять их противоречия, чтобы подобрать решение, которое будет для каждой из заинтересованных сторон нести больше выгоды, чем затрат.

Анализ существующей практики решения проблемы незаконного списания денежных средств

Чтобы разработать оптимальное решение проблемы, было решено проанализировать способы снижения количества случаев незаконного списания денежных средств с банковских карт при оплате услуг в сети Internet, которые существуют в отечественных банках на данный момент. Для анализа были выбраны Сбербанк, т. к. он является крупнейшим транснациональным и универсальным банком России, и Тинькофф, т. к. он представляет собой банк, который полностью отказался от отделений (все банковские операции мгновенно проводятся по телефону или через интернет).

В процессе общения с представителями данных банков выяснилось, что оба банка предлагают услуги страхования банковских карт, однако из-за множества оговорок о страховых случаях и дороговизны услуг, страхование не пользуется большим спросом у держателей карт.

Кроме страхования, для повышения безопасности банк Тинькофф предлагает при необходимости подключать бесплатную услугу «Операции в интернете», а после платежа снова отключать ее. Во время отключения данной услуги мошенники не могут производить операции по списанию средств держателей карт в сети Internet. В Сбербанке пока нет услуги, позволяющей временно отключать возможность осуществления операций в сети Internet по банковской карте.

Также в этих банках существует услуга открытия дополнительной виртуальной карты, которая в Тинькофф-банке осуществляется бесплатно, а в Сбербанке её стоимость составляет 60 рублей в год. В случае недоверия к ресурсу у потребителя появляется возможность не показывать настоящие реквизиты счета.

Таким образом, чтобы свести к минимуму риск несанкционированного списания денежных средств с банковской карты в сети Internet банки советуют потребителю регулировать активность услуги «Операции в интернете», использовать виртуальную карту

и устанавливать лимит на сумму покупки.

Также мы изучили еще один существующий в международной и отечественной практике способ борьбы с незаконным списанием денежных средств с банковских карт через интернет, им является чарджбек. Чарджбек (англ. chargeback) – это отмена транзакции, предназначенная для защиты потребителей от мошеннических действий, совершенных как продавцами, так и физическими лицами. Процедура чарджбека осуществляется следующим образом: держатель карты подает в банк-эмитент соответствующее заявление, в котором указывает причину, почему он считает операцию недействительной или мошеннической. Далее кредитная организация проводит расследование и в случае правоты заявителя списывает с торговой точки опротестованную сумму платежа и возвращает ее плательщику, т.е. чарджбек происходит за счет торговой точки. Вот некоторые из причин, по которым возможно инициировать чарджбек:

- операция произведена на сумму, отличную от стоимости покупки;
- с карточки списаны деньги за покупку, которую держатель карты не совершал;
- деньги со счета списаны, но покупатель не получил товар или услугу;
- покупатель не удовлетворен продуктом или сервисом, например, на деле товар отличается от того, что было обещано ранее продавцом, или услуги были оказаны не в полном объеме и т. д.

В случае отказа в виде формальной отписки, необходимо подать жалобу в банк. Официальная жалоба – это способ обратить на себя внимание, так как она подлежит регистрации, а в дальнейшем банк обязан принять какие-либо меры и отчитаться перед руководством.

Еще одним существующим методом борьбы с незаконным списанием средств является принцип работы некоторых глобальных виртуальных торговых площадок, таких как AliExpress. Он заключается в том, что переведенные денежные средства будут списываться с карты клиента в момент покупки, но поступают на счет продавца только при предоставлении товара (работ, услуг), либо по истечению определенного периода, установленного Банком.

На основании отечественного и международного опыта предлагаем следующие пути решения рассматриваемой в кейсе проблемы (описание каждого из решений, их преимущества и недостатки приведены в Приложении 1):

1. Усовершенствовать процедуру чарджбека, сделав его доступным и по кредитным картам.

2. Ввести функцию «доверяю продавцу».

3. Внести уточнения в ряд положений 161-ФЗ.

4. Внедрить процедуру кредитования по сниженной процентной ставке для пострадавших от незаконного списания денежных средств на время решения проблемы банком.

5. Сделать обязательной услугу «Виртуальная карта» для всех держателей карт.

После анализа преимуществ и недостатков каждого из предложенных решений проблемы было выбрано два наиболее оптимальных решения: внедрение кредитования по сниженной процентной ставке и ввод функции «доверяю продавцу».

Одним из наиболее оптимальных способов борьбы с незаконным списанием денежных средств в сети Internet было решено выбрать введение банками и интернет-магазинами функции «доверяю продавцу» в окна оплаты, поскольку применение данного способа на практике является наименее затратным и наиболее быстро внедряемым среди предложенных решений. Данная функция будет действовать по принципу работы глобальной виртуальной торговой площадки AliExpress. При всплывании окна оплаты клиенту будет дан выбор, когда списанные за покупку денежные средства поступят на счет продавцу: сразу или только после предоставления товара, или по истечении определенного периода, установленного Банком (данная процедура проиллюстрирована в Приложении 3). Если клиент выберет второй вариант, списанные с него деньги до момента предоставления товара или окончания определенного банком периода будут храниться в виртуальном хранилище банка-эквайера. Внедрение функции «Доверяю продавцу» позволит снизить риски, связанные с незаконным списанием денежных средств, а также риски, связанные со случаями непредоставления товара. К недостаткам данного решения можно отнести необходимые траты банков и интернет-магазинов на модернизацию окон оплаты, а также затраты банков на создание виртуального хранилища, в которое будут поступать денежные средства.

Внедрение кредитования по сниженной процентной ставке также было выделено, как одно из наиболее полезных нововведений по разрешению ситуаций с незаконным списанием средств (пошагово процесс предоставления клиенту возможности получения кредита по сниженной процентной ставке представлен в Приложении 2).

Данный способ борьбы с рассматриваемой проблемой не требует внесения изменений в законодательство, что является его преимуществом над другими разработанными решениями. Кроме того, он аналогичен предлагаемому нами процессу чарджбека по кредитным картам, однако обладает перед ним существенным преимуществом для клиентов в случае, если банк не может решить возникшую проблему.

В целом, суть данного кредитования заключается в том, что на время решения проблемы с мошенничеством по желанию клиента ему предоставляется кредит по сниженной процентной ставке. Если будет доказана невиновность клиента в незаконном списании денежных средств, то уплаченные по кредиту со сниженной процентной ставкой денежные средства будут перечислены на банковский счет потребителю вместе с ранее уплаченными по кредиту процентами. В случае если банк не может решить возникшую проблему, потерпевшему предоставляют кредит со сниженной процентной ставкой в качестве рефинансирования единовременным платежом образовавшейся задолженности с более высокой процентной ставкой.

Преимуществом данного способа также является возможность уменьшения кредитной зависимости, образовавшейся в результате действий мошенников.

К недостаткам можно отнести возможность использования такого кредита недобросовестными клиентами для обмана банка или кредитной организации, а также возникновение высокого уровня ответственности у банков и кредитных организаций.

Заключение

В процессе проведенного исследования нами была изучена проблема незаконного списания денежных средств с банковской карты.

Был проведен анализ действующей нормативной базы РФ, в которой рассматривается списание денежных средств с банковской карты, оплата услуг через интернет. В ходе анализа был обнаружен ряд положений, касающихся незаконного списания денежных средств с банковской карты при оплате услуг через интернет, которые требуют уточнения.

В процессе исследования проблемы были выявлены интересы стейкхолдеров, их противоречия и взаимная увязка.

Помимо этого, были изучены уже существующие способы урегулирования проблемы, а именно услуги, которые предоставляют банки для борьбы с незаконным списанием средств с карты; проведено их сравнение.

Рассмотрена процедура чарджбэка и принцип работы некоторых глобальных виртуальных торговых площадок, таких как AliExpress. На их основе разработан и предложен ряд способов повышения безопасности пользователей при совершении операций с банковскими картами в сети Internet. Среди них выявлены два наиболее выгодных методадля внедрения на практике: внедрение кредитования по сниженной процентной ставкой и ввод функции «Доверяю продавцу».

В заключение были даны ответы на вопросы по ситуации, описанной в кейсе (Приложение 5).

Можно отметить, что ежедневно возникают новые угрозы, которые не всегда можно предсказать, поэтому внесенные нами предложения не являются универсальными. Следовательно, исследования в данном направлении всегда будут оставаться востребованными и актуальными.

Список литературы

1. "О национальной платежной системе": Федер. закон Рос. Федерации, 27 июн. 2011 г., № 161 // Консультант Плюс Версия Проф. – Электрон. текстовые дан. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_115625/

2. "О некоторых вопросах практики рассмотрения споров, связанных с заключением, исполнением и расторжением договоров банковского счета": Постанов. Пленума ВАС Рос. Федерации, 27 сен. 2007 г., № 612 (ред. от 04. окт . 2012) // Консультант Плюс Версия Проф. – Электрон. текстовые дан. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_23458/

3. "Об утверждении Правил продажи товаров дистанционным способом": Постанов. Правит. Рос. Федерации, 27 сен. 2007 г., № 612 (ред. от 04.10.2012) // Консультант Плюс Версия Проф. – Электрон. текстовые дан. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_71418/

4. "Гражданский кодекс Российской Федерации (часть первая)" от 30. нояб. 1994 г. № 51-ФЗ (ред. от 03. авг. 2018 г.) (с изм. и доп., вступ. В силу с 01. янв. 2019 г.) – ст. 10 // Консультант Плюс Версия Проф. – Электрон. текстовые дан. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_5142/62129e15ab0e6008725f43d63284aef0bb12c2cf/

5. "Международный стандарт финансовой отчетности (IFRS) 3 "Объединения бизнесов": Приказ Минфина Рос. Федерации, 28. дек. 2015 № 217н) (ред. от 30. окт. 2018) (с изм. и доп., вступ. в силу с 01. янв. 2019) // Консультант Плюс Версия Проф. – Электрон. текстовые дан. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_9027/9e5d4849d8ca1f3cd88dff170479109e12b2f3be/

6. Безопасность в интернете: как защитить свои платежи? / Кибербезопасность // А. Мордвинцев. – Электрон. текстовые дан. – Журнал "Forbes", 2017. – Режим доступа:

https://www.forbes.ru/finansy-i-investicii/346943-bezopasnost-v-internete-kak-zashchitit-svoi-platezhi

7. Как воспользоваться бонусами от банков? / О. Николаенко. – Электрон. текстовые дан. – Интернет портал MOLNET.RU, 2018. – Режим доступа: https://www.molnet.ru/mos/ru/finace_investments_credits/o_479816. – СМИ Эл №ФС77 -36547 от 11 июня 2009 г.

8. Как нас обманывают карточные мошенники? / А. Еремена. – Электрон. текстовые дан. – Электрон. период. изд. «Ведомости», 2017. – Режим доступа: https://www.vedomosti.ru/finance/articles/2017/09/29/735855-kak-obmanivayut. – СМИ Эл № ФС77–26576

9. Конференции-2018 / Ф. Вирин, председат. сессий разл. конф.. – Электрон. текстовые дан. – Режим доступа: http://www.fedorvirin.ru/conference18/

10. Наличные и безналичные платежи / СБЕРБАНК. – Электрон. текстовые дан. – Июль, 2018. – Электрон. текстовые дан. – Режим доступа: https://www.sberbank.ru/common/img/uploaded/news/2018/cash_and_cashless_payments.pdf

11. Недешевые людские слабости: как воруют деньги с карт / С. Кракова. – Электрон. газет. – 2018. – Режим доступа: https://www.gazeta.ru/business/2018/11/15/12060103.shtml

12. Ответы на вопросы по применению статьи 9 Федерального закона «О национальной платежной системе» / Центральный Банк России. – Электрон. текстовые дан. – Режим доступа: http://www.cbr.ru/Content/Document/File/16195/faq_9.pdf

13. Официальный сайт Сбербанк: Банковские тренды 2018 / СберДанные. – Электрон. текстовые дан. – 25.31.2018. – Режим доступа: https://www.sberbank.ru/common/img/uploaded/files/pdf/analytics/bank_trends_2018.pdf

14. Программа "Цифровая экономика Российской Федерации": Распоряж. Правит. Рос. Федерации, от 28 июля 2017 г. № 1632-р. – Москва: 2018. – 88с. – Электрон. текстовые дан. – Режим доступа: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf

15. Результаты наблюдения в национальной платежной системе за 2016–2018 годы / Центр. Банк России. – Электрон. текстовые дан. – Режим доступа: http://www.cbr.ru/Content/Document/File/59588/results_2016-18.pdf

16. Сравнение норм Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» с международным опытом на примере законодательства США и норм Директивы 2007/64/ЕС, включая ее имплементацию на территории

Великобритании 1 / Центральный Банк России. – Электрон. текстовые дан. – Режим доступа: https://www.cbr.ru/PSystem/regulation_p/compare161/ – Интернет-приемная

Приложения

Приложение 1

Таблица 1 – Преимущества и недостатки разработанных предложений

№	Предложение	Субъект	Преимущества	Недостатки
1	**Обязать банки ввести виртуальные карты, у которых такие данные, как номер карты и cvc-код, будут отличаться от данных оригинальной банковской карты. Реквизиты по счету виртуальной карты должны соответствовать реквизитам банковской карты.**	**Клиент**	**Возможность обеспечения безопасности своих денежных средств от мошенничества в сети Internet. Снижение риска повторной оплаты дорогостоящего товара (работ, услуг), который достигается путем использования лимита перед каждой покупкой. Экономия денег и защита окружающей среды, так как для изготовления виртуальной карты не требуется пластик, который загрязняет окружающую среду**	**Ограниченная сфера применения**
		ЦБ Коммерческие Банки	**Значительное уменьшение числа обращений в банк для разрешения вопросов об интернет-мошенничестве**	**Затраты на создание сервиса**
		Регулятор	**Повышение уровня доверия граждан к отечественному банковскому сектору и содействие развитию цифровой экономики в России.**	**Затраты денежных средств и времени, связанные с изменением законодательства, для введения данного сервиса на обязательной основе**
2	**Предоставить клиенту возможность получения кредита по сниженной процентной ставке на время решения проблемы Банком (см. Приложение 2)**	**Клиент**	**Уменьшение кредитной зависимости, образовавшейся в результате действий мошенников**	**Возможность использования недобросовестными клиентами для обмана банка или кредитной организации**
		ЦБ Банки	**В случае вины потерпевшего банк все равно получит денежные средства обратно**	**Высокий уровень ответственности**

Продолжение Таблицы 1

№	Предложение	Субъект	Преимущества	Недостатки
3	Ввести функцию «Доверяю продавцу», которая будет действовать по принципу работы глобальной виртуальной торговой площадки AliExpress (см. Приложение 3)	Клиент	Снижение рисков, связанных со случаями непредоставления товара (работы, услуги)	Отсутствие недостатков
		ЦБ Коммерческие Банки	Снижение уровня мошенничества и повышение уровня доверия граждан	Траты на создание виртуального хранилища, в которое будут поступать денежные средства
4	Внести уточнение в ряд положений 161-ФЗ, а именно: - уточнить способ уведомления клиента о списании с его счёта денежных средств; - уточнить сроки оповещения и момент, в который уведомление об операции с использованием ЭСП считается полученным клиентом	Клиент	Улучшение положения в спорных моментах по мошенничеству	Установление данных положений может быть невыгодно для клиента
		ЦБ Коммерческие Банки		Финансовые затраты банков в случае принятия смс-уведомлений, как единственно верный способ
		Регулятор	Повышение уровня доверия граждан к отечественному банковскому сектору	Затраты денежных средств и времени, связанные с изменением законодательства для введения данного сервиса на обязательной основе
5	Предложение внедрить в отечественные банки процедуру Чарджбека по кредитным картам (см. Приложение 4)	Клиент	Высокая вероятность возврата денег клиенту	Есть вероятность получить отказ от банка
		ЦБ Коммерческие Банки	Повышение уровня доверия граждан к отечественному банковскому сектору	Процедура требует много времени

Источник: составлено авторами на основе выводов, данных в исследовании

Приложение 2

Детализация процесса предоставления клиенту возможности получения кредита по сниженной процентной ставке на время решения проблемы Банком в случае незаконного списания денежных средств с кредитной карты в сети Internet:

Шаг 1. Держатель карты связывается с эмитентом для подачи заявления по поводу конкретной транзакции.

Шаг 2. Эмитент рассматривает заявление и выносит решение о достоверности проблемы.

2.1 Недостоверная проблема – заявление держателя карты не удовлетворено, процесс возврата денежных средств завершается.

2.2 Достоверная проблема – процесс возврата денежных средств продолжается. На время решения проблемы клиенту (по его желанию) предоставляется кредит по сниженной процентной ставке в случае, если образовавшаяся в результате мошеннических действий задолженность превышает совокупный заработок клиента за последний год.

Шаг 3. Расследование проблемы эмитентом.

Шаг 4. Вынесение итогового решения банком:

4.1 Решение в пользу потребителя предполагает переход денежных средств из статуса кредита в статус денежных средств, возвращённых банком. Таким образом, незаконно списанные денежные средства будут перечислены на банковский счет потребителю вместе с ранее уплаченными по кредиту процентами.

4.2 В случае если банк не может решить возникшую проблему, потерпевшему предоставляют возможность использования предоставленного на Шаге 2 кредита в качестве рефинансирования единовременным платежом образовавшейся задолженности с более высокой процентной ставкой.

Таким образом, банки всё равно вернут свои денежные средства, а у клиента будет снижено кредитное бремя.

Данное решение наиболее подходит для разрешения проблемы, аналогичной той, что произошла с героем кейса.

Приложение 3

Подробнее про функцию «Доверяю продавцу»:

Внешний вид окна оплаты с предложенной нами функцией (см. Рисунок 1):

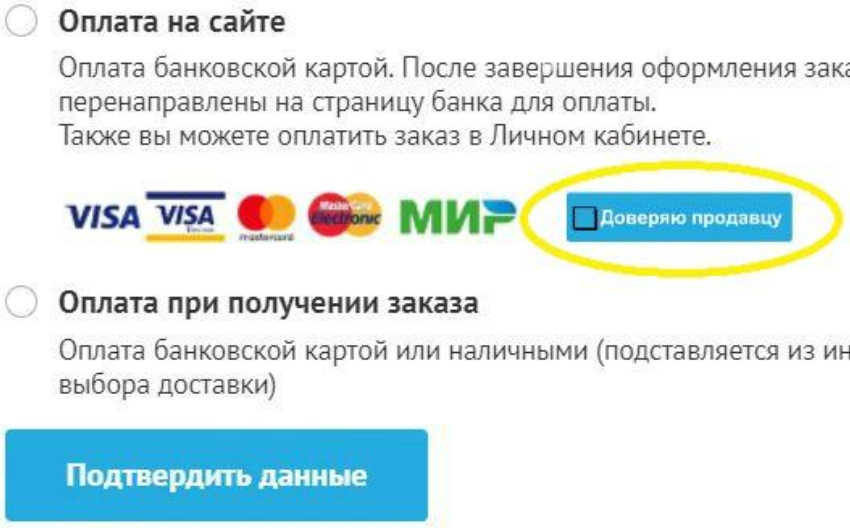

Рисунок 1 – Визуализация функции «Доверяю продавцу» (выделено жёлтым цветом)

Источник: разработано авторами на основе выводов, данных в исследовании

Если держатель карты доверяет продавцу, он ставит галочку (см. Рисунок 2) и деньги переходят продавцу сразу после оплаты:

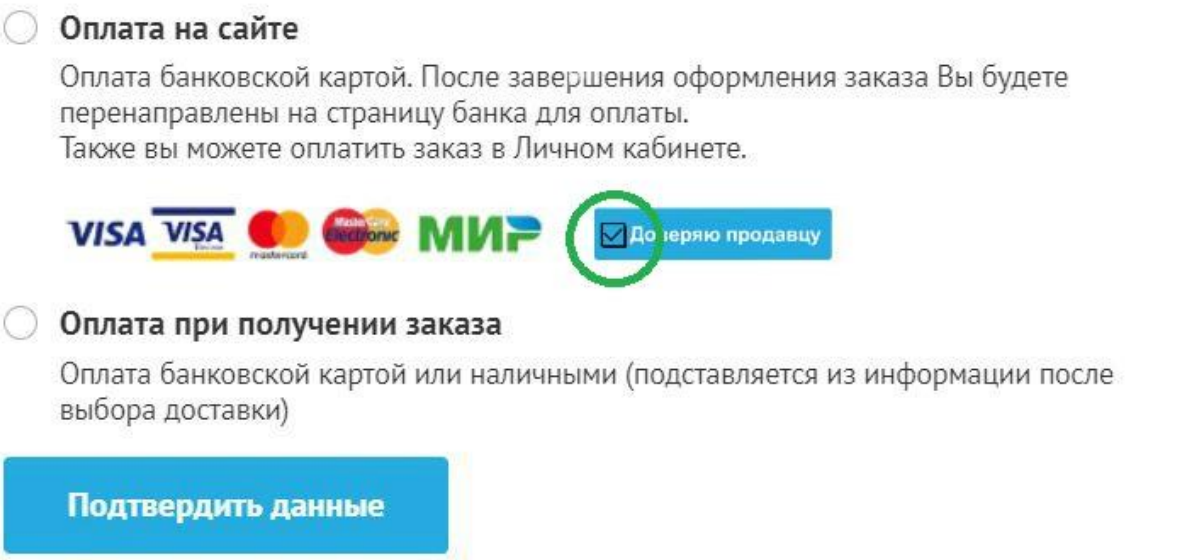

Рисунок 2 – Наглядный пример использования функции «Доверяю продавцу» (отмечено зеленым цветом)

Источник: разработано авторами на основе выводов, данных в исследовании

Если держатель карты не доверяет продавцу, он оставляет поле пустым (см. Рисунок 3), и деньги переходят в виртуальное хранилище банка, где и находятся до того момента, как клиент получит товар либо по истечении срока, установленного Банком:

Рисунок 3 – Наглядный пример использования функции «Доверяю продавцу» в случае недоверия продавцу (отмечено красным цветом)

Источник: разработано авторами на основе выводов, данных в исследовании

Приложение 4

Нами было проведено исследование уже существующей процедуры чарджбек в отечественных банках. Рассмотрением жалоб по незаконному списанию средств с банковских карт занимаются специалисты особого профиля. Упор в их работе делается на то, чтобы сохранить лояльность клиента. Поэтому сотрудники, обрабатывающие жалобы, на уровне кодекса корпоративной этики остаются на стороне клиента. Также преимуществом чарджбека является длительное время на подачу заявления для его проведения. Сравнение сроков обращения для проведения чарджбека в разных российских банках отражено на Рисунке 4.

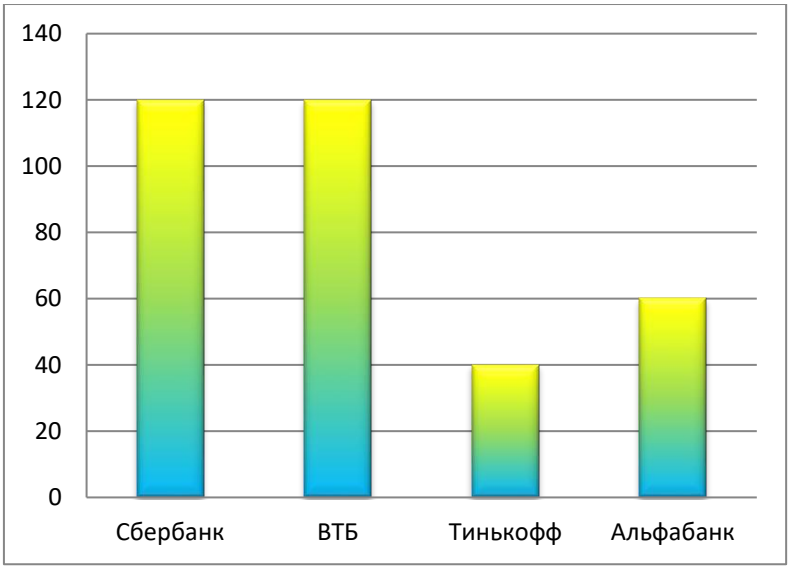

Рисунок 4 - Срок обращения для проведения процедуры чарджбека, в днях

Источник: составлено авторами на основе данных с официальных сайтов банков

В целом, отношение банков к чарджбеку неоднозначное. Все финансовые организации работают с международной платежной системой, а значит должны четко следовать их предписаниям. Недостатком является тот факт, что более 90% сотрудников разных банков либо уточняют регламент принятия заявления, либо отправляют к другому специалисту, либо отказываются принять заявление.

Ни один из банков, с представителями которых мы общались, не смог дать нам четкого ответа по вопросу наличия чарджбека по кредитным картам. Исходя из этого, мы предлагаем ввести услугу «Чарджбек по кредитным картам», которая значительно бы

снизила процент нерешенных дел по мошенничеству с банковскими картами в сети Internet. Она будет идентична процедуре по дебетовым картам, однако из-за того, что при кредитовании возникает обязанность уплачивать проценты за пользование кредитом, а также начисляется пеня при просрочке платежей, возникает вопрос, в каком порядке и при каких условиях данные платежи должны будут выплачены держателем карты. Процесс решения этого вопроса будет аналогичен процессу по предоставлению клиенту возможности получения кредита по сниженной процентной ставке, который был рассмотрен в Приложении 2, но в случае если банк не может решить возникшую проблему, потерпевший будет должен вернуть кредит, однако без начисления пени за просроченный платеж.

Приложение 5

Ответы на вопросы кейса

Вопросы:

1) Должен ли герой кейса в данной ситуации оплачивать кредитную задолженность?

До вынесения судебного решения потерпевшему необходимо выплачивать кредит, чтобы избежать образования пеней в случае неудовлетворения его жалобы в суде.

Что он может предпринять, чтобы выиграть спор с банком?

Способы воздействия на банк:

- досудебная претензия на имя Председателя Правления Банка;
- жалоба в ЦБ РФ и финансовому омбудсмену;
- жалоба в Федеральную службу по надзору в сфере защиты прав потребителей;
- жалоба в ПС VISA/MasterCard о несоблюдении их правил;
- обращение в региональные и федеральные СМИ, в том числе и в сети Internet, что придаст данному вопросу общественных характер.

2) Как может потребитель финансовых услуг обезопасить себя от подобных ситуаций при покупке товаров и услуг в Интернете?

Бесплатно: устанавливать лимит, пользоваться виртуальной картой, использовать услугу «Операции в интернете», читать отзывы о сайте.

Платно: услуги страхования.

Какими характеристиками должна обладать страница оплаты, поддерживаемая добросовестной организацией?

Залогом надежности сайта являются:

1. Протокол SSL – Secure Socked Layer. Сайты, использующие SSL, передают зашифрованные данные по протоколу HTTPS, расшифровать которые можно с помощью специального секретного ключа. Это отличает их от незащищенных сайтов, использующих обыкновенный протокол HTTP. Адрес защищенного сайта должен начинаться с https://. Также рядом с адресной строкой должна быть иконка в виде закрытого замка. Эти знаки покажут, что вы имеете дело с ответственным продавцом, и ваши данные будут передаваться в зашифрованном виде.

2. Стандарты защиты информации PCI DSS (Payment Card Industry Data Security Standard), разработанные международными платежными системами, защищают данные банковских карт.

3. Технология 3-D Secure, которая позволяет проверять личность держателя карты в реальном времени. Обычно такая проверка проходит при помощи СМС. При введении присланного кода из СМС вы подтверждаете свою личность, после чего банк разрешает проведение транзакции. На сайте гарантом надежности будет служить надпись Verified by Visa или MasterCard Securecode.

4. Использование платежных систем PayPal или ApplePay, которые сами авторизуют и идентифицируют клиента, что снижает риск утечки информации о банковской карте.

5. Наличие антифрод-системы, которая оценивает финансовые операции онлайн и способна обнаружить сомнительные. Подобные системы-платформы способны предотвратить списание денег, если есть подозрение на мошенничество. Каждая операция, проходя через платформу, анализируется, после чего дается рекомендация отклонить или применить дополнительную проверку.

6. Установление только легальных расширений для браузера, которые можно скачать из официального магазина.

7. Подключение интернет-банка и смс-оповещения, что позволит отслеживать операции в режиме реального времени.

8. Открытие отдельной карты для интернет-платежей и использование ее для хранения незначительных денежных остатков.

9. Сохранение данных своей банковской карты в секрете от других лиц, в том числе от банковских служащих и от работников интернет-магазинов.

10. Совершение покупок с устройств, на которых установлена антивирусная защита.

11. Блокировка доступа к телефону паролем. Банки также рекомендуют не пользоваться услугами интернет-банков через обозреватель мобильного телефона, если на него приходит СМС-сообщение с подтверждающим одноразовым паролем[14].

Существуют и другие способы защиты своих денежные средств при оплате через Интернет.

В случае если покупатель не уверен в надежности интернет-магазина, возможно совершение платежа с помощью виртуальной карты, которая сразу после оплаты становится недействительной. Все, чем рискует покупатель – это средства на карте.

Также многие банки в своих онлайн-приложениях предлагают методы пассивной защиты. К примеру, они дают возможность клиентам скрывать из видимости счета. В этом

[14] http://www.forbes.ru/finansy-i-investicii/346943-bezopasnost-v-internete-kak-zashchitit-svoi-platezhi

случае мошенник, войдя в ваш онлайн-кабинет, не увидит вклад на крупную сумму денег или кредитную карту[15].

Необходимо соблюдать бдительность при просмотре оформления сайта. Поддельный обычно недостаточно проработан: мало контента и отсутствует архив. Нужно осторожно относиться к предложениям несуществующих магазинов о суперпродажах, специальных акциях, выгодных условиях покупки товаров, особенно брендовых и дорогих услуг, например, авиаперелетов[16].

Исходя из положений ст. 9 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе», банк несет ответственность, т. е. обязан выплатить сумму спорной транзакции в трех случаях:

1) банком не было направлено уведомление клиенту о совершении операции, и при этом операция была совершена без согласия клиента (ч. 13 ст. 9);

2) банк уведомил клиента о совершении операции, и клиент своевременно уведомил банк об утрате электронного средства платежа или его использовании без его согласия;

3) банк также обязан возместить стоимость транзакций, произведенных банком после получения уведомления об утрате электронного средства платежа или его использования в отсутствие согласия клиента (ч. 12 ст. 9).

3) Каким образом банки и регулятор могут содействовать повышению безопасности платежных операций в интернете (в том числе в ситуациях, когда внешние признаки сомнительных операций отсутствуют)?

См. Приложение 1

Нужны ли для этого какие-либо изменения в законодательстве?

Внести уточнение в ряд положений 161-ФЗ «О национальной платежной системе», а именно:

– уточнить способ уведомления клиента о списании с его счёта денежных средств;

– уточнить сроки оповещения;

– уточнить момент, в котором уведомление об операции с использованием ЭСП считается полученным клиентом.

[15] https://www.molnet.ru/mos/ru/finace_investments_credits/o_497996
[16] https://www.vedomosti.ru/finance/articles/2017/09/29/735855-kak-obmanivayut#/galleries/140737493571634/normal/1