

МОШЕННИЧЕСТВО КАК ИНТЕРНАЦИОНАЛЬНАЯ ПРОБЛЕМА

Доника Д.А.

Волгоградская академия МВД РФ, г.Волгоград

Россия, e-mail: ddd1993ddd@yandex.ru

В статье обсуждается проблема мошенничества с использованием банковских карт. Современное общество все больше становится «безналичным». Во всем мире широко используют пластиковые платежные карты. Они являются частью инструментов ежедневных операций на финансовых рынках. В связи с этим статистика преступлений, связанных с мошенничеством в этой области, характеризуется стойкой тенденцией к росту. Интернет-кражи с банковских карт россиян составляют 90% всех незаконных списаний с карт, остальное — это офлайн-кражи, скимминг и т.д. Учитывая, что за рубежом безналичный расчет имеет более длительную историю, представляет интерес оценка данного вида преступлений в международном интернет пространстве, что и явилось целью работы. В работе использованы результаты контент-анализа документов государственных и общественных организаций, законодательных документов, материалов периодических изданий и электронных ресурсов тематических Интернет-сайтов по рассматриваемой проблеме. проведенный обзор литературы по рассматриваемой проблеме показал, что за рубежом, как и в России, наблюдаются тенденции к росту мошенничества, связанного с безналичными расчетами. Во многом этому способствует рост технологий и развитие сети Интернет. Наиболее опасной проблемой, связанной с данным видом преступлений, является его способствование финансированию терроризма, через механизмы «отмывания денег». Поскольку, как показал последний печальный опыт террористических атак, проблема терроризма носит интернациональный характер, то и мероприятия профилактики в этой сфере должны проходить в рамках международного сотрудничества. Необходимо использовать международный опыт для предотвращения интеграции новых схем в национальное поле и создания надежных превентивных механизмов в законодательной сфере.

Ключевые слова: мошенничество, уголовное право, кредитные карты, финансирование терроризма.

FRAUD AS AN INTERNATIONAL PROBLEM

Donika D.A.

Volgograd Academy of the Ministry of Internal Affairs of the Russian Federation, Volgograd

Russia, e-mail: ddd1993ddd @yandex.ru

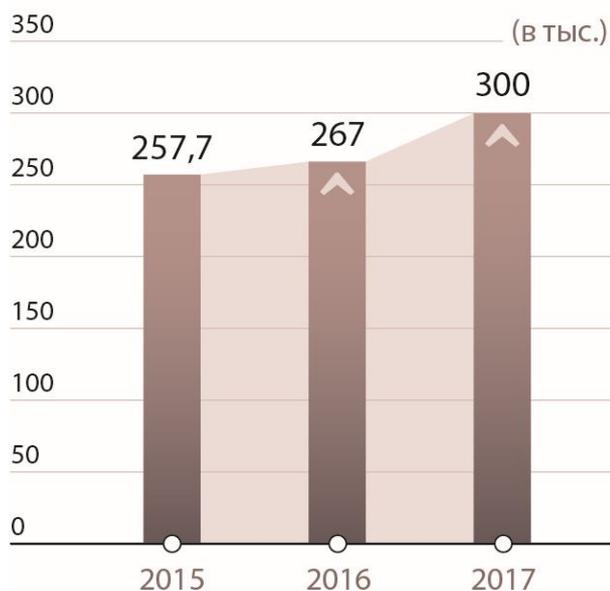
The article discusses the problem of fraud with the use of bank cards. Modern society is increasingly becoming non-cash. Plastic payment cards are widely used throughout the world. They are part of the tools of daily operations in financial markets. In this regard, the statistics of crimes related to fraud in this area, is characterized by a strong upward trend. Internet theft from Russian bank cards makes up 90% of all illegal card debits, the rest is offline theft, skimming, etc. Considering that abroad non-cash payments have a longer history, it is of interest to evaluate this type of crime in the international Internet space, which was the purpose of the work. The paper uses the results of a content analysis of documents of state and public organizations, legislative documents, materials of periodicals and electronic resources of thematic Internet sites on the problem under consideration. A review of the literature on the problem in question showed that abroad, as in Russia, there are trends towards an increase in fraud associated with non-cash payments. In many

ways, this is facilitated by the growth of technology and the development of the Internet. The most dangerous problem associated with this type of crime is its contribution to the financing of terrorism, through money laundering mechanisms. Since, as the last sad experience of terrorist attacks has shown, the problem of terrorism is international in nature, then preventive measures in this area should be carried out within the framework of international cooperation. It is necessary to use international experience to prevent the integration of new schemes into the national field and create reliable preventive mechanisms in the legislative sphere.

Keywords: fraud, criminal law, credit cards, terrorist financing.

Актуальность. Современное общество все больше становится «безналичным». Во всем мире широко используют пластиковые платежные карты [1,2,3]. Они являются частью инструментов ежедневных операций на финансовых рынках. В связи с этим статистика преступлений, связанных с мошенничеством в этой области, характеризуется стойкой тенденцией к росту. Согласно обзору ЦБ, за 2014 год со счетов граждан незаконно списывали деньги 300 тыс. раз, общая сумма ущерба составила 3,5 млрд руб. С кредитных карт граждан мошенники списали 1,58 млрд руб., причем в 68% случаев для проведения транзакций мошенники использовали реквизиты чужих карт, в 21% случаев злоумышленники изготавливали поддельные карты, 11% несанкционированных списаний произошли по утерянным и украденным картам [3]. Большую часть суммы (свыше 1 млрд руб.) мошенники украли через интернет-банк и мобильное приложение. Объем неправомерных транзакций, совершаемых через дистанционные каналы обслуживания, вырос на 44,8%. Как говорится в исследовании компании «Информзащита», число интернет-краж с карт в 2017 году достигло 300 тыс., а объем ущерба — 1,05 млрд рублей (рис.1). Годом ранее мошенники скомпрометировали 267 тыс. карт, ущерб составил 1,08 млрд рублей (257,7 тыс. и 1,78 млрд рублей в 2015 году) [4]. Интернет-кражи с банковских карт составляют 90% всех незаконных списаний с карт, остальное — это офлайн-кражи, скимминг и т.д. В компании «Атак киллер», специализирующейся на кибербезопасности, подтвердили корректность данных оценок.

Число интернет-краж с банковских карт



Источник: «Информзащита»



Рис.1 Динамика интернет-краж с банковских карт в России с 2015 по 2017 г [4]

Учитывая, что за рубежом безналичный расчет имеет более длительную историю, представляет интерес оценка данного вида преступлений в международном интернет пространстве, что и явилось **целью** нашей работы.

Материалы и методы. В работе использованы результаты контент-анализа документов государственных и общественных организаций, законодательных документов, материалов периодических изданий и электронных ресурсов тематических Интернет-сайтов по рассматриваемой проблеме.

Полученные результаты и их обсуждение. Мошенничество с кредитными картами, как правило, представляет собой действие, совершенное любым лицом, которое с целью обмана в своих корыстных целях использует кредитную карту, которая была отозвана, аннулирована, заявлена как потерянная или украденная. Использование номера кредитной карты без фактического владения картой также является формой мошенничества с кредитными картами. Кража персональных данных для получения кредитной карты является еще одной более угрожающей формой мошенничества с кредитными картами, поскольку она работает в сочетании с кражей личных данных. Согласно обзору международных источников по данной проблеме, мошенничество с кредитными картами - это проблема, которая затрагивает всю индустрию потребительских кредитов. Это один из самых быстрорастущих видов мошенничества и один из самых трудных для предотвращения.

Первой возобновляемой кредитной картой, получившей универсальное согласие продавца, была BankAmeriCard, первоначально выпущенная в 1958 году Банком Америки.

Первая банковская карта была выпущена в Калифорнии. В 1966 году Bank of America расширил свою программу банковских карт, сформировав BankAmeriCard Service Corporation, которая лицензировала банки за пределами Калифорнии и позволяла им выпускать карты своим клиентам. К 1969 году большинство региональных банков преобразовали свои независимые программы в BankAmeriCard или Master Charge (теперь известные как VISA и MasterCard соответственно). К 1970 году более 1400 банков предложили ту или иную кредитную карту.

В начале 1970-х годов, когда для совершения покупки использовалась кредитная карта, она обрабатывалась вручную с помощью слайд-машины, которая оставляла отпечаток номера кредитной карты в чеке, состоящем из нескольких частей. Оригинальная копия была для продавца, а точная копия - для покупателя. Технологические достижения привели к тому, что большинство продаж по кредитным картам осуществлялось в электронном виде по телефону, компьютеру или через Интернет, а информация обрабатывалась в считанные секунды. Со времен ручных станков до современных электронных процессоров кредитные карты использовались мошенниками.

Одним из самых ранних способов совершения мошенничества с кредитными картами была либо кража карты из чьего-либо кошелька, либо «погружение в мусорное ведро» для получения копий квитанций с кредитных карт. Использование этих двух методов сократилось с появлением электронной обработки кредитных карт. Один из самых простых способов получить информацию об учетной записи человека или фактическую кредитную карту - это кража по почте. Через почтовые данные мошенник может иметь доступ к чьей-либо личной информации (включая номера счетов кредитных карт, кредитные лимиты и банковскую информацию) и использовать эту информацию для получения дополнительных карт или создания новых учетных записей без ведома истинного владельца.

Наиболее распространенным видом мошенничества в этой сфере являются предоплаты. Федеральные правила потребительского кредитования требуют, чтобы эмитенты кредитных карт зачисляли средства на счет клиента сразу после получения платежа. Теперь это возможно мгновенно, так как большинство транзакций являются электронными. Используя поддельную или украденную кредитную карту или номер кредитной карты, мошенник либо вносит предоплату на карту, либо переплачивает существующий баланс с помощью поддельного чека. Поскольку счет зачисляется при получении платежа, денежные авансы могут быть немедленно сняты с кредитной карты до того, как платеж будет очищен. Таким образом, мошенник может снять огромные суммы и останется незамеченным, пока не придет следующий счет.

Другим видом мошенничества с кредитными картами является подделка кредитных карт. Преступники с относительной легкостью смогли использовать технологию для изготовления мошеннических версий существующих кредитных карт, благодаря Интернету. Некоторые преступники продают магнитные полосы, найденные на картах, или технологию, позволяющую дублировать информацию с действующей кредитной карты. Эти магнитные полосы содержат всю информацию, которая нужна мошеннику: имена, номера счетов, кредитные лимиты, а также другую идентифицирующую информацию. Используя компьютерную систему и соответствующее оборудование, фальшивомонетчик может легко создать мошенническую кредитную карту. Мошенники также используют технологии для создания фиктивных карточек. Вымышленные карты более выгодны, потому что нет человека, действительно ответственного за учетную запись. Компании-эмитенты кредитных карт заметят, что аккаунт не оплачивается, и попытаются связаться с владельцем аккаунта, но никто не существует.

Многие финансовые учреждения выиграли от создания функций безопасности, предназначенных для предотвращения мошенничества, таких как голограммы, защитные коды (известные как коды проверки кредитных карт или идентификационные коды карт) и встроенные микрочипы. Тем не менее, поскольку потребители начали делать покупки по почте, по телефону и через Интернет, мошенничество росло в геометрической прогрессии. Там нет клерка, чтобы проверить кредитную карту в этих транзакциях. Это создает почти анонимную атмосферу, в которой легко использовать мошеннические карты или номера.

Представляют интерес, в плане прогноза роста рассматриваемых преступлений в России, выявленные за рубежом, так называемые «связанные проблемы». Одной из проблем, связанных с мошенничеством с кредитными картами, является двойственность потребителя. Агентства кредитных карт рекламируют нулевую ответственность за мошенничество с кредитными картами. В некоторых случаях может взиматься плата в размере 50 долларов США, но от нее также можно отказаться. Если чья-то кредитная карта утеряна или украдена, и об этом сообщается, клиент не несет ответственности за любые мошеннические платежи. Относительно легко узнать, была ли ваша карта потеряна или украдена; Вы больше не обладаете этим. Однако, если чей-то номер кредитной карты был украден и продублирован, это может быть неочевидным, если агентство кредитных карт не заметит необычную активность и не уведомит потребителя, если потребитель случайно проверит учетную запись в Интернете, или не поступит счет с мошенническими платежами. Некоторые преступники даже зашли так далеко, что сменили почтовый адрес на карточке, чтобы не быть пойманным потребителем, что продлевает время использования карточки. Однако многие преступники

просто используют номер, чтобы подать заявку на новую кредитную карту, которая прикреплена к имени потребителя, хотя он или она не будут знать о ее существовании.

После манипуляций мошенниками с кредитными картами у потребителя (собственника карты) могут возникнуть и отсроченные проблемы. Когда кредитная карта выдается на чье-то имя, это появляется в его или ее кредитном отчете. Если эта кредитная карта затем используется мошенническим путем, это также появляется в кредитном отчете и может иметь некоторые очень серьезные последствия, особенно если владелец карты совершенно не знает, что счет был открыт. Коллекторские агентства и кредиторы будут искать оплату, таким образом, ищет кого-то, кто сделает эти платежи. Большинство людей даже не осознают, что на их имена открыты другие счета, пока они не готовы совершить крупную покупку, например, машину или дом. Выполняется обычная проверка кредитоспособности, и потребители удивляются, когда им отказывают в получении ссуды на покупку автомобиля или ипотеки из-за их «плохого» кредита.

В США существует закон о выставлении счетов «справедливым» кредитам, который устанавливает порядок устранения ошибок при выставлении счетов на счета кредитных карт. Потребитель обязан связаться с кредитными агентствами, чтобы воспользоваться защитой прав потребителей. Во многих случаях кредитным агентствам требуются годы для расследования мошеннических действий; в то же время, автокредит или ипотека могут быть отсрочены или полностью отклонены. Один из лучших превентивных методов для обеспечения безопасности кредитной истории - это связаться с тремя кредитными бюро (Equifax, Experia).

Другая, актуальная проблема, связанная с данным видом мошенничества – «отмывание денег», под которым понимают процесс, при котором средства, полученные в результате противоправного поведения, приобретают очевидную легитимность - по сути, очищая преступные доходы. Финансирование терроризма - это процесс, с помощью которого средства собираются и используются для террористической деятельности. Попытки отмывания денег и финансирования терроризма могут быть направлены не только на международную торговую деятельность - деятельность местного бизнеса также может быть в опасности.

В Великобритании Национальное агентство по борьбе с преступностью (NCA), HM налоговой и таможенной службы (HMRC), другие правоохранительные органы, регулирующие органы и профессиональные организации работают вместе для борьбы с отмыванием денег. В некоторых секторах, таких как финансовые услуги, предприятия, занимающиеся денежным обслуживанием, бухгалтерские, юридические, агентства по недвижимости, поставщики трастовых и корпоративных услуг, крупные дилеры и казино,

юридические обязательства вытекают из Положений 2007 года о борьбе с отмыванием денег и Закона 2002 года о доходах от преступлений - «Proceeds of Crime Act 2002» (ПОСА), а также Закона о финансировании терроризма) [6].

Согласно ПОСА, все, кто работает в регулируемых секторах, у которых есть разумные основания для подозрений, должны сообщать о своих подозрениях или знании об отмывании денег в НСА. Отказ от сообщения является уголовным преступлением.

ПОСА также применяется к любому лицу, не входящему в регулируемый сектор, которое знает или подозревает или имеет разумные основания знать или подозревать, что другое лицо занимается отмыванием денег; и что информация поступала к ним в ходе его профессии, профессии, бизнеса или работы.

Поскольку Малайзия быстро превращается в крупный финансовый и туристический центр, она все больше становится уязвимой для мошенничества с кредитными картами. В 2014 году в Малайзии в обращении находилось около 6,2 миллиона кредитных карт, было зарегистрировано 204 случая по сравнению с 244 случаями в 2013 году. Что касается заявленных денежных потерь, то их объем увеличился с 721 704,58 миллионов долларов в 2013 году до приблизительно 4 799 021,51 миллионов долларов. В последние несколько лет банковская индустрия в Малайзии понесла огромные убытки мошенникам по кредитным картам из-за устройств для прослушивания телефонных разговоров. Мошенники даже модифицировали цифровые диктофоны или MP3-плееры для прослушивания телефонных линий. В связи с этой деятельностью по скиммингу Департамент по расследованию коммерческих преступлений (CCID) начал тесно сотрудничать с Центральным банком Малайзии, чтобы заставить финансовые учреждения выпускать чип-карты Еигорау, Mastercard и Visa (EMV) и шифровать все данные кредитных карт. Большинство банков начали выдавать чип-карты EMV в середине 2014 года, а также шифрование, и все банки выполнили эти инструкции. К концу 205 года все кредитные карты, выпущенные банками, соответствовали требованиям EMV. Внедрения дали очень обнадеживающие результаты и позволили сократить количество мошеннических операций с кредитными картами в Малайзии на 93% в 2015 году по сравнению с 2014 годом. CCID также предвидит, что некоторые мошенники по кредитным картам Малайзии будут мигрировать в соседние страны для осуществления своей незаконной деятельности. Таким образом, крайне важно, чтобы региональные правоохранительные органы и полицейские органы Азиатско-Тихоокеанского региона усиливали существующую тесную связь и оказывали взаимную помощь в борьбе с преступностью.

Заключение и выводы. Таким образом, проведенный обзор литературы по рассматриваемой проблеме показал, что за рубежом, как и в России, наблюдаются тенденции

к росту мошенничества, связанного с безналичными расчетами. Во многом этому способствует рост технологий и развитие сети Интернет. Наиболее опасной проблемой, связанной с данным видом преступлений, является его способствование финансированию терроризма, через механизмы «отмывания денег». Поскольку, как показал последний печальный опыт террористических атак, проблема терроризма носит интернациональный характер, то и мероприятия профилактики в этой сфере должны проходить в рамках международного сотрудничества. Необходимо использовать международный опыт для предотвращения интеграции новых схем в национальное поле и создания надежных превентивных механизмов в законодательной сфере.

Список литературы

1. Доника Д.А. Мошенничество в проблемном поле уголовного права // Международный студенческий научный вестник. - 2015. - № 4-4.- С. 663.
2. Доника Д.А. Современные тенденции толкования национального законодательства // Успехи современного естествознания. - 2012.- № 4. - С. 201-202.
3. Доника А.Д. Медицинское право: европейские традиции и международные тенденции // Биоэтика. - № 2(10) – 2012. - С.54-55.
4. Число интернет-краж с пластиковых карт выросло. [Электронный ресурс]: Режим доступа: <https://iz.ru/713533/anastasiia-alekseevskikh/vorovat-dengi-s-kart-stali-chashche-no-berut-menshe>. (Дата обращения: 10.0.2019).
5. ЦБ раскрыл объем мошеннических списаний со счетов россиян в 2014 году. [Электронный ресурс]: Режим доступа: <https://www.rbc.ru/finances/23/06/2015/558936aa9a79477bdc5736ec> (Дата обращения: 10.0.2019).
6. Debra E. Ross Crime and fraud prevention for businesses in international trade [Электронный ресурс]: Режим доступа: <https://sovetadvokatov.ru/238-moshennichestvo-v-internete.html>(Дата обращения: 10.0.2019).