

DOI 10.24412/1829-0485-2026-1-94-118
УДК 34.4414

Поступила: 27.04.2025г.
Сдана на рецензию: 28.04.2025г.
Подписана к печати: 16.02.2026г.

МОШЕННИЧЕСТВА В СФЕРЕ БЕЗНАЛИЧНЫХ РАСЧЕТОВ: ГРАЖДАНСКО-ПРАВОВЫЕ ПРОБЛЕМЫ И ПУТИ ИХ РАЗРЕШЕНИЯ

Р.А. Амирова

*Российско-Армянский университет
rozaamirova@mail.ru
ORCID: 0009-0009-2839-480X*

АННОТАЦИЯ

В данной статье исследуется правовое регулирование использования дистанционных каналов банковского обслуживания и электронных средств платежа в контексте безналичных расчетов, а также анализируются правовые последствия мошеннических действий, совершаемых в данной цифровой среде. Особое внимание уделено вопросам распределения ответственности за убытки, возникающие при несанкционированном доступе третьих лиц к счетам клиентов и правовым рискам неблагоприятных последствий таких действий. Рассмотрена возможность возврата денежных средств банком при выявлении признаков мошенничества, а также правомерность списания средств со счета клиента без его согласия. Сделан вывод о несоответствии отдельных положений договоров между банками и клиентами национальному законодательству, что может ослабить защиту прав собственности. Нами предложены меры по совершенствованию правового регулирования для повышения безопасности операций с банковскими картами и защиты интересов клиентов.

Ключевые слова: защита персональных данных, мошеннические операции, безналичные расчеты, право собственности, информирование.

Появление и повсеместное внедрение систем дистанционного банковского обслуживания способствовало динамичному развитию глобальной цифровой экономики, оптимизировав расчетные сети, повысив конкурентоспособность банков и расширив кредитные возможности финансовых институтов. Однако такая технологическая трансформация неизбежно привела бы к росту преступности в финансовой сфере. Это обусловлено как цифровой и финансовой неграмотностью части населения, так и уязвимостью программных интерфейсов банковских систем в сочетании с объективными трудностями правоохранительных органов при расследовании высокотехнологичных киберпреступлений.

Мошенничество в сфере безналичных расчетов сегодня является одной из наиболее опасных и динамично развивающихся форм хищения, характеризующейся высокой латентностью и сложностью раскрытия. Это связано с применением современных технологий, высокой квалификацией преступников и их специализированными знаниями, а также глобальной распространенностью преступной деятельности, что усложняет процесс доказывания. В связи с ростом случаев мошенничества, разнообразием механизмов преступлений и их негативным воздействием на финансовое благополучие граждан и репутацию кредитных организаций, актуальным становится определение правовых последствий действий сторон, вовлеченных в такие схемы, с обращением к нормам гражданского права, регулирующим обязательства, сделки и вопросы возмещения ущерба.

Современные угрозы утечек персональных данных через даркнет, такие как взломы серверов или недобросовестность сотрудников, способствуют росту мошенничества, включая социальный инжиниринг, оформление кредитов на имя жертвы или фальшивые сборы (например, сбор средств на лечение якобы родственника в социальных сетях или просьбы занять деньги у друзей). Для обеспечения безопасности операций в электронной форме важную роль играют средства идентификации, такие как пароли, PIN-коды, одноразовые SMS-коды, биометрия и цифровые сертификаты, которые служат цифровым аналогом подписи клиента.

Согласно Гражданскому кодексу Республики Армения (далее также – ГК РА), ключевыми положениями для удостоверения распоряжений денежными средствами являются:

1. **Обязанности банка:** по договору банковского счета банк обязан исполнять распоряжения клиента о денежных операциях (ст. 912 ГК РА).

2. **Удостоверение распоряжений:** права на распоряжение средствами удостоверяются документами, включая электронные средства идентификации (ст. 915 ГК РА).

3. **Использование электронных средств идентификации:** решение Кассационного суда от 05.08.2014 г. по гражданскому делу № ԵՄԴ/0426/02/13 подтверждает, что банк обязан исполнять распоряжения, заверенные электронными средствами идентификации, такие как пароли и коды, при операциях через банкоматы, POS-терминалы и интернет-банкинг. Код клиента, применяемый в таких случаях, считается достаточным доказательством полномочий для выполнения операций [1].

4. **Пределы обязательств банка:** банк не может ограничивать распоряжение средствами, если это не установлено законом или договором.

Таким образом, договор банковского счета предоставляет сторонам возможность предусмотреть в договоре удостоверение прав на распоряжение денежными средствами на банковском счете в электронной форме. При этом

такое удостоверение должно осуществляться с использованием средств идентификации, подтверждающих, что распоряжение дано уполномоченным лицом. К таким средствам идентификации могут относиться подпись клиента, кодовые слова, а также иные способы аутентификации. Указанные нормы и судебная практика подчеркивают важность обеспечения безопасных и надежных средств идентификации в договоре банковского счета.

Эффективность средств идентификации зависит от их технической сложности и способности противостоять современным угрозам, включая фишинг, взломы и социальную инженерию. Поэтому их разработка и использование должны соответствовать современным стандартам информационной безопасности и регулироваться договорными условиями, а также требованиями законодательства.

Платежная карта классифицируется как платежный инструмент, с помощью которого выполняются операции по снятию наличных денежных средств и безналичные транзакции [2]. При использовании платежной карты распоряжения клиента, переданные банку, считаются подтвержденными, если они содержат идентификационный код клиента, задействованный в электронных системах [3],[4].

Согласно пункту 18 Положения Совета Центрального банка Республики Армения №300-Н «О порядке установления правил безопасности, направленных на защиту интересов держателей карт в связи с выпуском, обслуживанием и распространением платежных карт, а также осуществлением операций с использованием платежных карт на территории РА» от 4 ноября 2014г. при использовании платежных карт в виртуальной среде (интернет) (за исключением виртуальных карт, созданных в системе «АрКа») эмитенты и обслуживающие банки обязаны обеспечивать защиту держателей карт и пользователей. Для этого применяются современные системы безопасности, соответствующие международным стандартам, такие как шифрование данных с использованием закрытых ключей 3D Secure или генерация одноразовых кодов.

Итак, при предоставлении услуг с использованием платежных карт в виртуальной/интернет-среде банки обязаны обеспечивать обслуживание операций через системы безопасности с целью исключения совершения несанкционированных транзакций, а также в соответствии с пунктом 3 подпункта 121 Правил 4 «Минимальных условий осуществления внутреннего контроля в банках», утвержденных решением Центрального банка № 102-Н от 18 апреля 2013 г. обязаны внедрять процедуры мониторинга и контроля операций, осуществляемых с использованием платежных карт, в том числе процедуры мониторинга поведения владельцев платежных карточек, уведомления держателей карт о совершаемых транзакциях, оперативного реагирования на инциденты в режиме реального времени, в случае если имеют место потеря карты, блокирование, отказ в обслуживании, конфискация средств банкоматом и так

далее, а также гарантировать круглосуточную доступность систем мониторинга и оповещения [5].

Из-за недостаточности правового регулирования на законодательном уровне в отношении выдачи, использования и обслуживания банковских карт, особенно важную роль в этих вопросах играют локальные акты банков, которые, как правило, называются «Правилами выпуска и обслуживания банковских карт» или «Общими условиями предоставления банковских услуг» и включают широкий спектр информации, касающейся всех аспектов взаимодействия – от процесса выдачи карты до расторжения договора между клиентом и банком.

В основном согласно типовым условиям банк не несет ответственности за убытки и ущерб, которые клиент может понести при использовании системы. Это включает, но не ограничивает следующие ситуации: несоблюдение условий безопасности при использовании системы, а также в случае передачи или обеспечения доступа третьим лицам устройств, используемых клиентом для входа в систему и работы с ней (мобильные телефоны, компьютеры и т.д.). Клиент обязан не передавать третьим лицам программное обеспечение системы, устройства для доступа к ней, а также пароли и коды. В случае умышленного или неосторожного предоставления доступа третьим лицам, клиент, как правило, несет полную ответственность за любые убытки, причиненные Банку и/или третьим лицам, а также за риски неблагоприятных последствий, которые могут возникнуть для него в связи с доступом третьих лиц.

Получается, что согласно основным типовым условиям банковского обслуживания, являющихся неотъемлемой частью договора, банк не несет ответственности за последствия, возникшие в результате несоблюдения клиентом требований безопасности при эксплуатации системы. Весь риск, связанный с использованием карты, OTP-кода, PIN-кода, CVV/CVC-кода, пароля карты и любой другой информации о карте ложится на держателя карты.

Статья 17 Гражданского кодекса РФ формулирует принцип полного возмещения убытков, который является основой гражданско-правовой ответственности. Лицо, чье право было нарушено, вправе требовать возмещения всех убытков, если договором или законом не установлены особые условия, ограничивающие размер возмещения. Это важная правовая норма, потому что направлена на восстановление справедливости и компенсацию потерпевшему всех расходов, понесенных из-за нарушения его прав. Во второй части данной статьи дано определение убытков, которые включают: реальный ущерб, ущерб в виде утраты или повреждения имущества, упущенную выгоду и нематериальный ущерб. Важно, что данное определение имеет универсальный характер и применяется в случае нарушения любого вида прав (например, в контексте договорных отношений или деликтных нарушений).

Статья 1058 ГК РА закрепляет обязанность возмещения ущерба в случае его причинения как личности, так и имуществу в полном объеме лицом, причинившим вред. Это общая норма, которая распространяется на различные виды вреда, включая вред от действий, нарушающих обязательства, и причинение ущерба в иных сферах гражданских правоотношений. Вторая часть устанавливает возможность освобождения лица от ответственности, если оно докажет, что вред был причинен не по его вине. Это исключение из общего принципа ответственности и предполагает необходимость доказательства отсутствия вины.

Таким образом, обе статьи работают в связке, где статья 1058 регулирует общие основания ответственности за вред, а статья 17 уточняет, что именно представляет собой ущерб и как он должен быть компенсирован.

Считаем, что банк должен нести ответственность за убытки клиента в случаях, когда нарушение со стороны банка привело к несанкционированным операциям, и эти операции могли быть предотвращены при должном уровне обслуживания и соблюдении обязательств банка. Таким примером может служить ситуация, когда, например, клиент своевременно сообщил о потере или краже карты, а банк не заблокировал карту в разумный срок, что привело к списанию денежных средств мошенниками. Однако чтобы банк нес ответственность, необходимо доказать, что:

1. Клиент своевременно сообщил банку о потере карты или подозрении на мошенничество.
2. Банк не выполнил свои обязательства по блокировке карты или принял недостаточные меры для предотвращения несанкционированных операций.
3. Убытки клиента непосредственно связаны с несвоевременной или ненадлежащей реакцией банка.

Кассационный суд Республики Армения, толкуя общие условия возмещения ущерба, неоднократно в своих решениях отмечал, что обязательным условием для возмещения ущерба является одновременное наличие следующих факторов: противоправное поведение должника, наличие ущерба, причинно-следственная связь между ущербом и ненадлежащим поведением, а также вина ответчика. При этом, в случае отсутствия хотя бы одного из указанных условий, ущерб не подлежит возмещению, за исключением случаев, предусмотренных законом [6].

В то же время, п. 1 статьи 1088 ГК устанавливает, что ущерб, причиненный гражданину в результате структурных, составных или иных дефектов услуг, а также вследствие предоставления неточной или недостаточно точной информации о таких услугах, подлежит возмещению со стороны поставщика этих услуг, независимо от наличия его вины и от существования договорных отношений с пострадавшей стороной.

Согласно п. 20 Положения Совета ЦБ РА №300-Н от 4-ого ноября 2014г. «О порядке установления правил безопасности, направленных на защиту интересов держателей карт в связи с выпуском, обслуживанием и распространением платежных карт, а также осуществлением операций с использованием платежных карт на территории РА», эмитент обязан постоянно обеспечивать наличие системы оповещения для быстрого реагирования на инциденты, связанные с платежной картой (потеря карты, блокировка, отказ в обслуживании, изъятие банкоматом и другие), а также ее круглосуточное (24/7) обслуживание в режиме реального времени [7].

Получается, что ущерб, причиненный физическому лицу в результате структурных, составных или иных дефектов услуг, а также вследствие предоставления неточной или недостаточно точной информации о таких услугах, подлежит возмещению со стороны поставщика этих услуг в случае, если будет доказано наличие причинно-следственной связи между недостатками услуг или предоставлением неточной или недостаточно точной информации о таких услугах и возникновением имущественного ущерба. Следовательно, банк может быть обязан возместить убытки клиента, если его действия или бездействие привели к несанкционированным списаниям, а также в случае, если банк не выполнил свои обязательства по обеспечению защиты денежных средств клиента. Например, если во время совершения операций клиент пытался связаться с банком по телефону для блокировки своей карты и предотвращения дальнейших несанкционированных операций, но звонок остался без ответа или был задержан, что позволило злоумышленнику совершить операции, ответственность за указанные убытки возлагается на банк.

Клиент имеет право выбрать любой из способов связи с банком для блокировки банковской карты. В свою очередь, банк обязан обеспечить наличие надлежащей процедуры, позволяющей клиенту установить связь с ним выбранным им способом и осуществить блокировку банковской карты.

Таким образом, если клиент выбирает, например, круглосуточный телефонный номер банка для блокировки своей банковской карты, банк обязан обеспечить незамедлительное установление связи с клиентом и начало процедуры блокировки карты. Это обусловлено положениями п. 3 статьи 417 и п. 1 статьи 1088 Гражданского кодекса, в соответствии с которыми банк несет ответственность за нарушение своей обязанности предоставить возможность связи для блокировки карты, независимо от наличия или отсутствия его вины.

В РФ Банк обязан информировать клиента о совершении *каждой операции* с использованием электронного средства платежа, направляя соответствующее уведомление в порядке, установленном *договором с клиентом* [8]. Если злоумышленники похитили средства с карты, а банк не уведомил клиента о проведенных операциях, то банк обязан компенсировать ущерб. Согласно Федеральному закон от 27.06.2011 N 161-ФЗ (ред. от 08.08.2024г.) «О

национальной платежной системе», банк обязан вернуть снятую сумму без согласия клиента, если выполнены следующие два условия:

1. Клиент сообщил банку о краже средств с карты *не позднее, чем на следующий день* после получения уведомления от банка о подозрительной транзакции. При получении уведомления о приостановлении операции до зачисления средств на банковский счет получателя, оператор по переводу денежных средств обязан приостановить зачисление на срок до пяти рабочих дней, уведомив получателя о необходимости представить документы, подтверждающие обоснованность получения средств. Если документы не предоставлены, Банк обязан вернуть средства Клиенту в течение двух рабочих дней.

2. При использовании карты не были нарушены правила безопасности. В частности, клиент не предоставил данные карты, не хранил PIN-код вместе с картой, не записывал код на карте и не разрешал никому копировать или фотографировать карту [9].

Если банк сможет доказать обратное, то похищенная сумма не будет возвращена.

В соответствии с п. 21 Приложения «О порядке установления правил безопасности, направленных на защиту интересов держателей карт в связи с выпуском, обслуживанием, распространением платежных карт и осуществлением операций с платежными картами на территории Республики Армения», эмитент обязан незамедлительно информировать держателя карты о выполнении каждой операции с использованием платежной карты посредством короткого сообщения (SMS) в случае, *если держатель карты выразил желание воспользоваться данной услугой*.

При этом, в случае мошенничества, риск мошенничества не может быть возложен:

1. исключительно на держателя карты, если последний дал согласие на предоставление услуги информирования, но эмитент не обеспечил незамедлительное информирование посредством короткого сообщения (SMS);

2. исключительно на эмитента, если, после незамедлительного уведомления держателя карты о совершенной операции посредством короткого сообщения (SMS), держатель карты не предпринял предусмотренных данным Порядком, Договором или основными правилами выполнения операций с использованием платежных карт профилактических мер (например, не уведомил незамедлительно о выполнении операции либо об ее отсутствии с его стороны) (...) [10].

Существующее правовое регулирование содержит ряд проблемных аспектов и пробелов, в частности отсутствие унифицированных механизмов информирования клиентов. Согласно ч. 4 ст. 9 Федерального закона № 161-ФЗ, порядок информирования определяется договором, что приводит к вариативности подходов между банками. В Российской Федерации банки обязаны

информировать клиента о каждой транзакции, тогда как в Республике Армения при отказе от услуги информирования все негативные последствия возлагаются на держателя карты. При отсутствии унифицированных стандартов информирования клиенты могут оказаться в неравных условиях. Например, один банк может предусмотреть уведомление исключительно через личный кабинет, другой – через SMS, а третий – по электронной почте. Это может стать причиной пропущенных уведомлений и, как следствие, негативных последствий для клиентов.

Следующая проблема связана с неоднозначностью определения «несанкционированных операций»: законодательство недостаточно четко определяет критерии, по которым операция может быть признана несанкционированной, что может вызывать споры между банками и клиентами. Кроме того, клиенты остаются в уязвимом положении, оператор освобождается от ответственности, если клиент нарушил порядок использования ЭСП. Однако доказательство нарушения часто требует сложной экспертизы.

В соответствии с разъяснениями Пленума ВС РФ обязанность доказывания соблюдения всех необходимых требований к банковским операциям лежит исключительно на самом банке [11]. Обязанность доказать правомерность списания денежных средств (в частности поступление соответствующего распоряжения именно от клиента) лежит на банке (определения КГД ВС РФ от 28 апреля 2015г. № 18-КГ15-48, от 7 февраля 2017г. № 5-КГ16-228).

Эта правовая позиция вполне обоснована, поскольку в тех случаях, когда клиент утверждает, что он не совершал распоряжения, на основании которого осуществлено списание денежных средств со счета, возложение бремени доказывания на него означало бы существенную тяжесть доказывания отрицательного факта. Вопреки распространенному заблуждению, отрицательные факты доказывать можно, но в некоторых случаях настолько затруднительно, что несправедливо возлагать это бремя на соответствующее лицо. Банк же, напротив, вполне может защищать свой интерес, предъявив суду доказательство совершения владельцем счета надлежащего распоряжения. Если банк не может доказать, что списание денежных средств со счета клиента было надлежащим (т.е. произошедшим на основании распоряжения клиента), клиент вправе требовать привлечения его к ответственности [12].

Более того, по нашему мнению, даже если клиент по неосторожности передал злоумышленнику свои персональные данные, а затем своевременно предпринял попытки связаться с банком для блокировки своей карты, это может рассматриваться как ситуация, при которой первоначально было совершено нарушение со стороны держателя карты, а впоследствии клиент попытался устранить его последствия. Однако, если на момент уведомления банка злоумышленники уже распорядились денежными средствами, ответственность клиента сохраняется в части, связанной с его неосторожностью, но банк

может нести ответственность за убытки, если не обеспечил надлежащий мониторинг транзакций или не принял мер для предотвращения дальнейших списаний. Например, если банк не уведомил клиента о подозрительной операции или не приостановил ее, это может быть основанием для возмещения убытков. Таким образом, распределение ответственности зависит от конкретных обстоятельств, включая момент уведомления, действия банка и наличие причинно-следственной связи между неосторожностью клиента и убытками.

Хотелось бы обратить внимание на два, как нам кажется, практикообразующих решения Верховного Суда РФ в части переноса бремени ответственности с клиента на саму кредитную организацию. Верховный Суд РФ в постановлении от 17 января 2023г. по делу №5-КГ22-121-К2 отменил решения нижестоящих судов, отказавшихся признать кредитный договор ничтожным [13]. Дело касалось обмана гражданки Е., которая, введя коды из СМС по указанию мошенников, фактически одобрила индивидуальные условия кредита и перевод средств. Верховный Суд указал на необходимость исследования ключевых обстоятельств, включая проверку принадлежности счета, назначения СМС с кодами, содержания заявки на кредит и логики действий кредитной организации при обработке операций.

В деле №5-КГ22-127-К2 Верховный Суд РФ отменил решения нижестоящих судов, отказавших в признании кредитного договора ничтожным, и направил дело на новое рассмотрение. Преступник, получив доступ к мобильному приложению клиента АО «Тинькофф Банк», оформил кредит и перевел средства на свой счет. Суд указал на необходимость оценки формы и условий кредитного договора, переписки клиента с банком и факта немедленного перевода средств на счет третьего лица. [14]

Верховный Суд РФ впервые занял сторону клиентов в делах о мошенничестве при оформлении кредитов, что, вероятно, связано с определением Конституционного Суда РФ от 13.10.2022 № 2669-0. КС РФ подчеркнул, что обман как основание для оспаривания сделок подтверждается общими правилами доказывания. При дистанционном оформлении кредитов банкам предписано принимать повышенные меры предосторожности, особенно в случаях, когда кредит оформляется на клиента, а средства сразу перечисляются третьим лицам [15].

В современной судебной практике наиболее сложной является ситуация, когда технические системы банка фиксируют корректный ввод кодов аутентификации, в то время как клиент заявляет о совершении операции злоумышленниками. В подобных случаях возникает риск необоснованного возложения на потребителя бремени доказывания так называемого «отрицательного факта» (факта отсутствия волеизъявления на совершение операции), что в условиях цифровых расчетов практически неосуществимо для непрофессионального участника.

Представляется, что в таких спорах суду следует исходить из принципа процессуального выравнивания сторон, применяя стандарт доказывания «баланс вероятностей». Учитывая профессиональный статус банка и его техническое превосходство, обязанность доказывания должна распределяться следующим образом: как сторона, контролирующая информационную систему, банк обязан представить не только формальный протокол ввода кода, но и доказательства надлежащей работы антифрод-системы. Суду необходимо оценить «цифровой след» транзакции: использовался ли типичный для клиента IP-адрес и идентификатор устройства, не фиксировалось ли подозрительное использование программ для удаленного доступа (например, “AnyDesk” или “TeamViewer”). Если параметры операции (сумма, время, получатель) резко отклонялись от привычного профиля потребления клиента, отсутствие дополнительной верификации со стороны банка должно интерпретироваться как несоблюдение обязанности по обеспечению безопасности услуги. Потребитель, в свою очередь, должен подтвердить добросовестность своего поведения доступными ему средствами. К ним относятся «косвенные доказательства»: немедленное обращение в правоохранительные органы, предоставление устройства для технической экспертизы на предмет отсутствия вредоносного ПО, а также доказательства невозможности совершения операции лично (например, данные геолокации или свидетельские показания о нахождении в ином месте).

Такой подход позволяет избежать формализма, при котором наличие «правильного кода» автоматически легализует любую мошенническую операцию, и стимулирует банки к совершенствованию систем превентивного мониторинга.

В соответствии с Директивой Европейского парламента и Совета 2015/2366/ЕС о платежных услугах (PSD2) банки обязаны принимать меры для предотвращения мошенничества и могут *приостанавливать* или отменять платежи при наличии обоснованных подозрений на мошенничество. В частности, статья 71 PSD2 устанавливает, что поставщики платежных услуг должны принимать меры для предотвращения мошенничества и обеспечения безопасности платежных операций. Кроме того, статья 72 PSD2 предусматривает, что поставщики платежных услуг могут приостанавливать или отменять платежные операции, если у них есть обоснованные подозрения на мошенничество [16].

Проблемным является вопрос о том, является ли обязанностью или правом банка возврат денежных средств отправителю в случае возникновения подозрения на мошеннический характер перевода. Для реализации этого права в РА в настоящее время существует практика пересмотра условий договоров между банком и клиентами, включая пункт, содержание которого, по нашему мнению, представляется несколько спорным. Согласно этому пункту «Банк имеет право по своему усмотрению приостановить возможность распоряжения, владения и использования средствами на счете клиента и/или

средствами, зачисленных на него, а также (...) без дополнительного поручения клиента перевести эти средства на сторону, осуществляющую перевод (в том числе, списав их со счета клиента с учетом установленной комиссии за посредничество), если банк располагает информацией или подозрениями, что средства, переведенные или зачисленные на счет клиента, могут быть частью мошеннической, поддельной или фиктивной сделки или цепочки сделок, включая наличие данных, идентифицирующих проблемную операцию в отчетах о мошенничестве, полученных от местных/международных платежных систем или финансовых организаций (...)» [17].

Для разграничения понятий важно отметить, что приостановление операций (например, временная блокировка счета при подозрении на мошенничество) отличается от безакцептного списания. Приостановление предполагает сохранение средств на счете клиента до выяснения обстоятельств, тогда как списание влечет их фактическое изъятие, например, путем возврата отправителю или перечисления на другой счет. В контексте мошенничества безакцептное списание может применяться банком как мера реагирования на выявленные признаки мошеннической транзакции (например, перевод средств на счет, связанный с фишингом). Однако, как будет обосновано далее, такие действия противоречат ст. 922 ГК РА, которая допускает списание средств только на основании распоряжения клиента, решения суда, закона или договора, но не по одностороннему усмотрению банка, если это не связано с погашением задолженности клиента перед банком.

Анализируя ограничения права получателя денежных средств на распоряжение средствами, зачисленными на его банковский счет, следует отметить, что правомерность таких ограничений должна оцениваться в каждом конкретном случае с учетом соблюдения национальных законодательных норм, гарантирующих защиту права собственности.

Часть 1 статьи 60 Конституции РА устанавливает, что каждый имеет право на владение, пользование и распоряжение приобретенной на законном основании собственностью по своему усмотрению. Согласно части 3 той же статьи, право собственности может быть ограничено только законом – в целях защиты интересов общества или основных прав и свобод других лиц. В соответствии со статьей 75 Конституции РА, при регулировании основных прав и свобод законами устанавливаются организационные механизмы и процедуры, необходимые для эффективного осуществления этих прав и свобод [18].

Иначе говоря, основой регулирования права собственности в отраслевом законодательстве является Конституция, а специальные законы лишь определяют необходимые организационные механизмы и процедуры для реализации этого права.

Согласно статье 1 Протокола № 1 «Европейской конвенции о защите прав человека и основных свобод», каждое физическое или юридическое лицо имеет право на уважение своей собственности (...). Однако предыдущие положения не препятствуют государству применять такие законы, которые оно считает необходимыми для осуществления контроля за использованием собственности в соответствии с общими интересами. [19]

В этом контексте важно отметить, что Европейский суд по правам человека в своей прецедентной практике по многим делам признал, что ограничение прав лица на денежные средства, находящиеся на банковских счетах, квалифицируется как контроль за использованием собственности в смысле статьи 1 Протокола № 1 Конвенции. Следовательно, такой контроль должен быть основан на законе. [20]

Согласно договору банковского счета банк обязуется принимать и зачислять на открытый клиентом счет поступающие денежные средства, выполнять распоряжения клиента об осуществлении перечислений, выдаче соответствующих сумм со счета и осуществлении других операций по счету (часть 1 статьи 912 ГК РА).

Как частное проявление установленных в статье 60 Конституции прав клиента распоряжаться своими средствами, часть 3 статьи 912 ГК РА также закрепляет, что банк не вправе определять и контролировать направления использования денежных средств клиента или устанавливать не предусмотренные законом или договором банковского счета другие ограничения его права распоряжаться своими денежными средствами по своему усмотрению.

Конституционный суд, обращаясь к содержанию права собственности, закрепленного в статье 60 Конституции РА, указал, что выражение «по своему усмотрению» в этой норме подчеркивает, что реализация права собственности основывается на четко выраженной воле собственника, которая рассматривается как обязательное условие осуществления этого права [21].

В рамках данного анализа считаем крайне важным рассмотреть императивные законодательные положения, определяющие допустимые пределы ограничения права клиента распоряжаться, владеть и использовать свои денежные средства.

Так, согласно статье 926 ГК РА, озаглавленной «Недопустимость ограничения распоряжения счетом», не допускается ограничивать права клиента распоряжаться денежными средствами, находящимися на счете, за исключением наложения ареста на денежные средства, находящиеся на счете, или прекращения операций по счету в случаях, предусмотренных законом. Конституционный суд также выразил аналогичное правовое мнение о том, что ограничение права клиента распоряжаться денежными средствами на счете допустимо исключительно на основании закона [22]. Подобные интерпретации содержатся во множестве доктринальных источников права [23].

На основании вышеизложенного приходим к выводу, что право клиента распоряжаться денежными средствами на счете может быть ограничено только законом, как того требует часть 3 статьи 60 Конституции. Ограничение права собственности исключительно законом в целях защиты общественных интересов или основных прав и свобод других лиц, а также изъятие собственности только на основании судебного решения в предусмотренных законом случаях, являются ключевыми конституционными гарантиями неприкосновенности собственности [24].

В соответствии с логикой, изложенной в части 3 статьи 912 ГК РА, диспозитивное регулирование, касающееся возможности ограничения прав клиента на распоряжение денежными средствами на своем счете в договоре, не может толковаться так, что сторонам договора предоставляется возможность установить положения, которые нарушают саму сущность прав клиента на распоряжение средствами на счете. Когда речь идет о возможности ограничения прав клиента на распоряжение денежными средствами в договоре, не будет лишним сослаться на положение части 2 статьи 3 ГК РА, согласно которой гражданские права могут быть ограничены *только законом*, если это необходимо для защиты государственной и общественной безопасности, общественного порядка, здоровья и нравственности общества, защиты прав и свобод, чести и доброго имени других лиц. Наряду с этим регулированием, граждане и юридические лица свободны в установлении своих прав и обязательств на основании договора, определении любых условий, *не противоречащих законодательству*. То есть, стороны договора свободны в установлении своих прав и обязанностей в обязательственных правоотношениях, но это право должно реализовываться так, чтобы условия договора не противоречили внутреннему законодательству.

Следует отметить, что статьей 922 ГК РА исчерпывающе установлены основания для списания денежных средств со счета, а именно: 1) распоряжение клиента, 2) решение суда, 3) случаи, предусмотренные законом, и 4) случаи, предусмотренные договором между банком и клиентом для вывода средств.

Поскольку в рамках данного анализа рассмотрение случаев списания денежных средств со счета по первым трем основаниям не представляется целесообразным, основное внимание сосредоточено на четвертом основании – списании средств со счета в порядке, предусмотренном договором между банком и клиентом. Представляется важным изучить этот вопрос с учетом действующей практики в банковской системе Республики Армения.

В общем порядке статья 922 ГК РА применяется для правового регулирования процедур безакцептного и неоспоримого списания средств с банковских счетов. В рамках банковской практики положения о безакцептном списании средств можно встретить, в частности, в «Общих условиях предоставления банковских услуг», утвержденных приказом председателя отделения

ОАО «Ардшинбанк» от 23.05.2024 № 42-Л (пункты 3.16, 11.31, 12.20, 13.50) [25], в «Условиях предоставления и обслуживания платежных карт» ОАО «Акба Банк», вступивших в силу с 27 июля 2023 года (пункты 5.3, 7.7, 7.8 и другие) [26], в «Условиях обслуживания и правил использования платежных карт» ОАО «Америабанк» [27], утвержденных решением директоров от 08.07.2015 №03/17/15 (текущая редакция от 24.09.2024 №01/139/24) (пункт 7.6), в «Условиях предоставления услуг и правил» ОАО «ВТБ Банк Армения», утвержденных решением директоров от 07.08.2020 №237 (пункт 3.8) [28], в «Общих правилах открытия и обслуживания (управления) банковских и депозитных счетов» «Фаст Банк» ОАО (пункт 3.8) [29].

Конституционный суд, рассматривая вопрос о правомерности включения в договор условий, касающихся безакцептного и неоспоримого списания денежных средств, в контексте оценки, означает ли применение таких условий лишение лица собственности без учета его воли или без соблюдения гарантий, предусмотренных частью 4 статьи 60 Конституции, отметил следующее: во-первых, как уже обсуждалось выше, права клиента на распоряжение средствами на счете могут быть ограничены в случаях, предусмотренных законом, например, при наложении ареста на средства на счете или при приостановке операций по счету, во-вторых, в соответствии с прецедентным правом Европейского суда по правам человека, требование о взыскании долга не может рассматриваться как вмешательство в право на уважение собственности должника, поскольку долг не может быть расценен как «имущество» в смысле статьи 1 Протокола №1 (“*Cheminade v. France*” (Dec.), приложение №31599/96, 26.01.1999) [30].

На основании вышеизложенного можно заключить, что списание денежных средств со счета клиента без его согласия на основании положений о безакцептном списании, предусмотренных договором, считается правомерным только в случае направления выведенных средств на погашение задолженности клиента *перед тем же банком*. В противном случае часть 2 статьи 922 ГК РА не может быть корректно истолкована и применена, так как это приведет к нарушению конституционных гарантий, обеспечивающих неприкосновенность собственности.

По данному вопросу российская судебная практика является противоречивой. В ряде случаев условия о безакцептном списании денежных средств со счета клиента рассматриваются как противоречащие, в том числе положениям комментируемого пункта (Постановление ВС РФ от 22 декабря 2015г. № 303-АД15-14824). В то же время существует подход, согласно которому такие условия признаются законными и не ущемляющими права потребителя (Постановление ВС РФ от 9 августа 2016 г. № 307-АД16-9324; Определение КГД ВС РФ от 11 октября 2016г. № 59-КГ16-13).

Если абстрагироваться от вышеизложенного анализа о недопустимости ограничения права собственности клиента на денежные средства, необходимо подчеркнуть, что положение, предоставляющее банку право возвращать отправителю сумму, зачисленную на счет клиента, без его дополнительного распоряжения в случае подозрений о «мошенническом» характере транзакции, фактически не может быть реализовано на практике.

Основанием для этого вывода является тот факт, что понятия «мошеннический» и «мошенничество» в том смысле, в каком они обычно используются в банковской практике, равнозначны понятиям «преступный» и «преступление». Согласно этой логике, квалификация деяния как преступления, предусмотренного Уголовным кодексом Республики Армения, а также инициирование соответствующего производства по предполагаемым преступлениям однозначно выходит за пределы прав и обязанностей банков. То есть банк, очевидно, не является государственным органом или должностным лицом, наделенным соответствующими полномочиями в рамках Уголовно-процессуального кодекса Республики Армения. Поэтому и банк не вправе по своему усмотрению произвольно квалифицировать какую-либо транзакцию как «мошенническую» и осуществлять действия, вытекающие из такой квалификации (например, списание денежных средств, принадлежащих лицу, с его счета).

С другой стороны, законодатель, учитывая необходимость защиты общественной безопасности, экономических и финансовых систем Республики Армения от рисков, связанных с отмыванием денег и финансированием терроризма, и через установление правовых механизмов противодействия этим явлениям, преследует важнейшую цель – защиту от этих рисков. В этой связи, 26 мая 2008 года был принят Закон Республики Армения «О борьбе с отмыванием денег и финансированием терроризма».

Кратко рассматривая законодательные инструменты в рамках борьбы с отмыванием денег и финансированием терроризма, следует отметить, что тот же закон предусматривает строгие правовые нормы, касающиеся признания сделки или делового отношения подозрительными (статья 7), ограничения определенных типов сделок и операций (статья 15), надлежащего контроля за текущими деловыми отношениями (статья 17), приостановки подозрительных сделок или деловых отношений (статья 26), отказа в проведении сделок или прекращения деловых отношений (статья 27), а также замораживания имущества лиц, связанных с терроризмом или распространением оружия массового уничтожения (статья 28). Не вдаваясь в подробности процедур, предусмотренных рассматриваемым законом для выполнения отдельных действий, следует отметить, что ни одно из этих процедурных положений не наделяет Банк правом списывать средства, уже зачисленные на счета клиентов, на основании выполненного поручения и передавать их на счет отправителя. Более того, процедурные механизмы, предусмотренные законом, обеспечивают

прямой контроль Центрального банка за выполнением вышеуказанных действий и, в случае необходимости применения более строгих ограничений, привлечение органов оперативно-розыскной деятельности и публичных участников процесса.

Указанные правовые нормы преследуют конкретную цель – обеспечение общественной безопасности, с четким процессуальным порядком ограничения права собственности, соразмерным этой цели. К тому же, все эти ограничения предусмотрены законом, как того требует часть 3 статьи 60 Конституции.

На основе изложенного, в случаях возникновения у банков обоснованных сомнений относительно законности сделок, для предотвращения отмыывания денег предусмотрен четкий правовой процесс в соответствии с внутренним законодательством, и банк обязан воздерживаться от действий, противоречащих данному законодательству, принимая во внимание защиту прав на собственность, закрепленную законодательными гарантиями.

Учитывая вышеизложенные правовые позиции, считаем, что положение, предусмотренное в договоре между клиентом и банком, согласно которому банк на свое усмотрение может ограничить право клиента распоряжаться средствами, зачисленными на его счет, а также без дополнительного распоряжения клиента перевести эти средства на счет отправителя, если банк имеет информацию или подозрения о том, что зачисленные средства могут быть частью мошеннической сделки или цепочки сделок, не соответствует внутреннему законодательству.

Противоположное толкование основным выводам данного анализа ослабляет концепцию неприкосновенности собственности и подрывает правовой механизм, установленный внутренним законодательством для ее защиты.

Анализ существующих правовых норм как в РА, так и в зарубежных странах показывает, что законодательство о платежной системе и банковской деятельности направлено на обеспечение безопасности клиентов и их денежных средств. Однако выявлены проблемы, связанные с недостаточной унификацией подходов и сложностями в правоприменении. Для устранения указанных недостатков необходима корректировка нормативно-правовых актов с учетом текущих рисков и тенденций в финансовой сфере.

1. В частности, требуется установление *единых стандартов информирования клиентов*, включая минимальные временные рамки для оповещения клиентов об операциях.

2. Необходимо также расширить обязанности банков по контролю транзакций: закрепить *обязательство банков отслеживать подозрительные операции в реальном времени и оперативно информировать клиентов*. Например, в РФ 24 июля 2024г. вступил в силу федеральный закон [31], который обязывает банки тщательнее отслеживать операции своих клиентов. Специ-

альное подразделение Банка России – «ФинЦЕРТ» собирает данные коммерческих банков обо всех случаях, когда их клиенты сталкивались с мошенниками, и фиксирует их в специальной базе данных. С ней коммерческие банки обязаны сверяться, прежде чем давать согласие на проведение той или иной операции. Если выяснится, что банк одобрил транзакцию по реквизитам, которые фигурируют в базе данных «ФинЦЕРТа», он обязан будет вернуть деньги владельцу карты, даже если тот сам их перевел.

3. Кроме того, необходимо *усилить роль государственных органов в надзоре за операциями, проводимыми через национальную платежную систему*, и обеспечить более строгую ответственность за нарушение норм законодательства, касающихся защиты прав потребителей. Это потребует внедрения современных технологий мониторинга и анализа транзакций. Важно также создать условия для *эффективного взаимодействия между национальными и международными регуляторами*, чтобы обеспечить бесперебойную и безопасную работу платежных систем в условиях глобализации финансовых потоков. Опираясь на опыт РФ, стоит отметить, что сотрудники МВД России могут оперативно получать информацию о финансовых операциях без согласия клиента из автоматизированной системы «ФинЦЕРТ». Существует установленный механизм информационного обмена между ведомствами, что способствует усилению борьбы с кибермошенничеством. Благодаря системе «одного окна», получение данных, необходимых для расследования преступлений, возможно в максимально короткие сроки. Обмен информацией происходит с соблюдением требований банковской тайны. [32]

4. В условиях активного внедрения технологий искусственного интеллекта и блокчейн-технологий необходимо *разработать дополнительные меры по защите персональных данных*, а также определить четкие механизмы их обработки и хранения.

«Свою роль в предупреждении могут играть и банки, обеспечивая контроль за сомнительными операциями по счетам клиентов, а также их блокировку в таких случаях» [33]. СберБанк совместно с АБК разработал специальную функцию собственного оператора сотовой связи «СберМобайл», который с помощью искусственного интеллекта анализирует текст разговора и предупреждает пользователя о подозрении на мошенничество в процессе разговора. Данная система получила название «Аура» и является самообучающейся языковой нейросетевой моделью глубокого обучения, способной распознавать меняющуюся методику мошеннического обмана потерпевшего на основании тысяч разговоров настоящих мошенников [34].

Банк «Тинькофф» предлагает своим клиентам установить приложение, которое аналогичным образом будет отслеживать содержание разговоров с клиентом, сравнивать источник звонка и номер телефона с уже имеющейся в базе банка картотеке мошеннических номеров.

Для выявления мошеннических операций ОАО «Америабанк» разработало концепцию «доверенного устройства». Под «доверенным устройством» понимается устройство, с которого клиент впервые входит в свой аккаунт. Это означает, что при попытке входа в мобильный банкинг клиента с нового устройства (например, нового телефона или компьютера) клиент обязан связаться с банком для прохождения повторной идентификации. Такая мера направлена на предотвращение случаев мошенничества и защиту персональных данных клиента. Концепция «доверенного устройства» (“trusted device”) также применяется в «Конверс Банк» АОЗТ.

Анализируя современные механизмы обеспечения безопасности безналичных расчетов, необходимо рассмотреть практику внедрения банками технологических «фильтров» доступа. В частности, ЗАО «АйДи Банк» применяет правило автоматической временной блокировки доступа к системе дистанционного банковского обслуживания на срок до 4–5 часов при попытке входа с нового, нетипичного для клиента устройства. Оценивая данную меру, следует разрешить потенциальное противоречие между защитой права собственности и превентивными ограничениями распоряжения счетом. Представляется, что кратковременная блокировка доступа не является нарушением сущности конституционного права, если она отвечает критериям пропорциональности и правомерности. Ключевое правовое различие здесь заключается в разграничении приостановления операции и безакцептного списания средств. В рамках рассматриваемой процедуры денежные средства остаются на счете клиента, сохраняя статус-кво; банк не распоряжается ими в одностороннем порядке, а лишь фиксирует их положение до подтверждения воли титульного собственника.

С точки зрения гражданского права, такая практика квалифицируется не как «изъятие собственности», а как реализация банком обязанности по обеспечению сохранности имущества клиента. Данная мера представляет собой «технологическую паузу», необходимую для аутентификации субъекта права. Однако для сохранения правомерности такой блокировки банк обязан соблюдать два условия: немедленно предоставлять клиенту альтернативный канал верификации (видеозвонок, биометрическая идентификация или визит в офис) для оперативного снятия ограничений основывать блокировку на объективных признаках угрозы (например, нетипичный IP-адрес в сочетании с попыткой совершения резкой, нехарактерной транзакции).

При соблюдении указанных условий кратковременное ограничение доступа является примером добросовестного превентивного контроля, который не нарушает условий договора банковского счета, а, напротив, выступает эффективным инструментом защиты интересов потребителя в условиях высокотехнологичного мошенничества.

В ОАО «Ардшинбанк» при попытке входа с нового устройства на экране отображается QR-код, который необходимо сфотографировать с помощью

нового устройства. Этот механизм предназначен для дополнительной проверки и подтверждения подлинности устройства, используемого клиентом, что способствует повышению уровня безопасности учетной записи.

5. Предлагается *разработать четкие критерии для выявления мошеннических операций*. Например, такими критериями могут быть: наличие получателя средств в «черном списке» банка; совпадение характеристик устройства, используемого для входа в систему, с данными, зарегистрированными в базе банка как подозрительные; а также несоответствие характера, сумм, периодичности, местоположения или устройства владельца счета его типичной финансовой активности. Аналогичные критерии были утверждены приказом Банка России от 27 сентября 2018 года № ОД-25253 [35]. Однако, как показывает практика и статистика случаев мошенничества, многие банки не соблюдают данные рекомендации в полной мере. Это свидетельствует о необходимости усиления контроля за исполнением нормативных актов, а также повышения ответственности кредитных организаций за игнорирование установленных мер по противодействию мошенническим операциям.

6. Особое внимание необходимо уделить *повышению финансовой грамотности населения*. Обучение клиентов может включать проведение разъяснительных кампаний о том, что банки никогда не запрашивают конфиденциальные данные, такие как PIN-коды, CVC-коды или пароли. Например, в Нидерландах существует практика предотвращения повторных случаев мошенничества: Управление по финансовым рынкам Нидерландов, получив список жертв мошенничества, напрямую связывается с пострадавшими.

Регулярное информирование клиентов о распространенных схемах телефонного мошенничества через SMS, email и социальные сети поможет повысить уровень финансовых знаний и содействовать формированию более осознанного поведения. Это, в свою очередь, способствует эффективному управлению личными средствами, ведению предпринимательской деятельности, использованию различных финансовых продуктов и услуг, а также улучшению других аспектов финансовой жизни.

Таким образом, дальнейшее развитие законодательства в области национальной платежной системы и банковской деятельности должно быть направлено на создание гармоничной и безопасной правовой среды, которая будет способствовать не только защите интересов клиентов, но и стабильности финансовой системы в целом. Только оперативное устранение выявленных проблем и недостатков в организации виктимологической защиты жертв дистанционных хищений может эффективно остановить рост подобных преступлений.

ЛИТЕРАТУРА

1. Решение Кассационного суда от 05.08.2014г. по гражданскому делу № ЁЧԴ/0426/02/13.
2. Закон Республики Армения «О платежно-расчетных системах и платежно-расчетных организациях» от 24 ноября 2004 г. (с последними изменениями от 09 июня 2022 г.) (п. «жа», п. «е» ст. 3).
3. Там же.
4. Положение Совета Центрального банка Республики Армения № 300-Н «О порядке установления правил безопасности, направленных на защиту интересов держателей карт в связи с выпуском, обслуживанием и распространением платежных карт, а также осуществлением операций с использованием платежных карт на территории РА» от 4 ноября 2014г. (с последними изменениями от 26 июля 2022г.) (п. 5).
5. Решение Совета Центрального банка Республики Армения № 102-Н «Об утверждении положения 4 «Минимальные требования по осуществлению внутреннего контроля над банками» и отмене решения Совета Центрального банка Республики Армения номер 71-Н от 11-го марта 2008г. от 18 апреля 2013 года (с последними изменениями от 14 октября 2024г.).
6. Решение Кассационного суда от 07.04.2018 по делу «Армянские программы» ООО против Гагика Ованнисяна, гражданское дело № ЁԿԴԴ/3614/02/15.
7. Решение Совета Центрального банка Республики Армения № 102-Н «Об утверждении положения 4 «Минимальные требования по осуществлению внутреннего контроля над банками» и отмене решения Совета Центрального банка Республики Армения номер 71-Н от 11-го марта 2008г. от 18 апреля 2013 года (с последними изменениями от 14 октября 2024г.).
8. Федеральный закон «О национальной платежной системе» от 27 июня 2011 № 161-ФЗг. (с последними изменениями от 08 августа 2024г.) (ст. 11–15).
9. Там же.
10. Положение Совета Центрального банка Республики Армения № 300-Н «О порядке установления правил безопасности, направленных на защиту интересов держателей карт в связи с выпуском, обслуживанием и распространением платежных карт, а также осуществлением операций с использованием платежных карт на территории РА» от 4 ноября 2014г. (с последними изменениями от 26 июля 2022г.) (п. 5).
11. Постановление Пленума Верховного Суда РФ от 28 июня 2012г. № 17 «О рассмотрении судами гражданских дел по спорам о защите прав потребителей» // «Российская газета», № 156. 2012.
12. *Карпетов А.Г., Байбак В.В., Иванов О.М., Любимова М.А., Махалин И.Н., Павлов А.А., Сарбаш С.В., Ястржембский И.А.* Заем, кредит, факторинг, вклад и счет: Постатейный комментарий к статьям 807–860.15 Гражданского кодекса Российской Федерации М.: «Логос», 2019. С. 1027.
13. Определение Верховного Суда РФ от 17 января 2023г. №5-КГ22-121-К2. URL: <https://www.vsrfr.ru/stor/pdf.php?id=2211722> (дата обращения: 06.01.2025).
14. Определение Судебной коллегии по гражданским делам Верховного Суда Российской Федерации от 16.12.2022 № 5-КГ22-127-К2 // Законы, кодексы и нормативно-правовые акты Российской Федерации. URL: <https://legalacts.ru/sud/opredelenie-sudebnoi-kollegii-po-grazhdanskim-delam-verkhovnogo-suda-rossiiskoi-federatsii-ot-16122022-n5-kg22-127-k2/> (дата обращения: 06.01.2025).

15. Об отказе в принятии к рассмотрению жалобы гражданки Юшковой Ксении Андреевны на нарушение ее конституционных прав пунктом 2 статьи 179 Гражданского кодекса Российской Федерации: Определение Конституционного Суда РФ от 13.10.2022 № 2669-О // Законы, кодексы и нормативно-правовые акты Российской Федерации: [сайт]. URL: [https:// legalacts.ru/sud/opredelenie-konstitutsionnogo-suda-rfot-13102022-n-2669-o/](https://legalacts.ru/sud/opredelenie-konstitutsionnogo-suda-rfot-13102022-n-2669-o/) (дата обращения: 06.01.2025).
16. International Bank for Commerce and Development AD and Others v. Bulgaria, no. 7031/05, § 123, 2 June 2016, and BENet Praha, spol. s r.o. v. the Czech Republic, no. 33908/04, §§ 92-93, 24 February 2011, Yunusova and Yunusov v. Azerbaijan, no. 68817/14, § 167, 16.07.2020. URL: <https://hudoc.echr.coe.int/eng?i=001-203562>
17. Постановление Конституционного суда от 12 июня 2018 года № УЧН-1418 на основании заявления Армине Атоян, Айка Назиняна и Аркадия Варданяна о соответствии части 2 статьи 887 Гражданского кодекса Республики Армения Конституции Республики Армения. (п. 4.5).
18. Брагинский М.И., Витрянский В.В. Договорное право. Книга пятая. В двух томах. Том 2: Договоры о банковском вкладе, банковском счете; банковские расчеты. Конкурс, договоры об играх и пари. М.: «Статут», 2006. С. 273; Российское гражданское право. Учебник. В 2 т. Т. II: Обязательственное право / Отв. ред. Е.А. Суханов. 4-е изд., стереотип. М.: «Статут», 2015. С. 945; Гражданское право Республики Армения. Ч. II. 2-е изд., с изм. и доп. / Т. Барсегян, А. Айкянц, Г. Гараханян, С. Мегрян. Ер.: Изд-во ЕГУ, 2008. С. 430.
19. Протокол № 1 Европейской конвенции о защите прав человека и основных свобод от 20.03.1952. URL: <https://docs.cntd.ru/document/901867999> (дата обращения: 04.01.2025г.).
20. International Bank for Commerce and Development AD and Others v. Bulgaria, no. 7031/05, § 123, 2 June 2016, and BENet Praha, spol. s r.o. v. the Czech Republic, no. 33908/04, §§ 92-93, 24 February 2011, Yunusova and Yunusov v. Azerbaijan, no. 68817/14, § 167, 16.07.2020 Доступно по ссылке: <https://hudoc.echr.coe.int/eng?i=001-203562>
21. Постановление Конституционного суда от 12 июня 2018 года № УЧН-1418 на основании заявления Армине Атоян, Айка Назиняна и Аркадия Варданяна о соответствии части 2 статьи 887 Гражданского кодекса Республики Армения Конституции Республики Армения. (п. 4.5).
22. Там же.
23. Брагинский М.И., Витрянский В.В. Договорное право. Книга пятая. В двух томах. Том 2: Договоры о банковском вкладе, банковском счете; банковские расчеты. Конкурс, договоры об играх и пари. – М.: Статут, 2006, с. 273; Российское гражданское право. Учебник. В 2 т. Т. II: Обязательственное право / Отв. ред. Е.А. Суханов. 4-е изд., стереотип. М.: Статут, 2015. С. 945; Гражданское право Республики Армения. Ч. II. 2-е изд., с изм. и доп. / Т. Барсегян, А. Айкянц, Г. Гараханян, С. Мегрян. Ер.: Изд-во ЕГУ, 2008. С. 430.
24. Постановление Конституционного суда от 12 июня 2018 года № УЧН-1418 на основании заявления Армине Атоян, Айка Назиняна и Аркадия Варданяна о соответствии части 2 статьи 887 Гражданского кодекса Республики Армения Конституции Республики Армения. (п. 4.5).

25. «Արդշինբանկ» ՓԲԸ: Ընդհանուր դրույթներ: URL: https://website-api.ardshin-bank.am/files/documents/general-terms-arm-72b55f9a-483c-4076-83f4-cb270_a9f2ef5.pdf (дата обращения: 04.01.2025г.).
26. «ԱՇԲԱ ԲԱՆԿ» ԲԲԸ վճարային քարտերի տրամադրման և սպասարկման պայմաններ: URL: https://www.acba.am/files/eFO%2075-02-37.30_27.07.23.pdf (дата обращения: 04.01.2025г.).
27. «Ամերիաբանկ» ՓԲԸ վճարային քարտերի սպասարկման պայմաններ և օգտագործման կանոններ: URL: https://ameriabank.am/Portals/0/files/announcements/green/Cards_terms_and_condintions_23_arm.pdf (дата обращения: 04.01.2025г.).
28. «ՎՏԲ-Հայաստան Բանկ» ՓԲԸ կողմից ֆիզիկական անձանց մատուցվող ծառայությունների պայմաններ և կանոններ (հրապարակային օֆերտա): URL: https://www.vtb.am/img/content/main-cards/OFERTA_arm_08_02.pdf (дата обращения: 04.01.2025г.).
29. «Общие правила открытия и обслуживания (управления) банковских и депозитных счетов» ОАО «Фаст Банк». URL: fstaticimages.blob.core.windows.net/fbfiles/account-type/1/Բանկային_և_ավանդային_հաշիվների_բացման_և_վարման_կանոններ.pdf (дата обращения: 04.01.2025г.).
30. Постановление Конституционного суда от 12 июня 2018 года № УԴՈ-1418 на основании заявления Армине Атоян, Айка Назиняна и Аркадия Варданяна о соответствии части 2 статьи 887 Гражданского кодекса Республики Армения Конституции Республики Армения. (п. 4.5).
31. Федеральный закон РФ «О внесении изменений в отдельные законодательные акты Российской Федерации» № 340-ФЗ от 24 июля 2023г. URL: <http://publication.pravo.gov.ru/document/0001202307240024?index=1> (дата обращения: 05.01.2025г.).
32. «Между Банком России и МВД России начнется онлайн-обмен информацией о мошеннических операциях» // Сайт Банка России. URL: <https://www.cbr.ru/press/event/?id=17142> (дата обращения: 05.01.2025г.).
33. Ренецкая А.Л., Петрякова Л.А. Виктимологическая характеристика мошенничеств в банковской сфере (по материалам Сибирского федерального округа) // Всероссийский криминологический журнал. 2022. Т. 16, № 4. СС. 452-462. URL: <https://doi.org/10.17150/2500-4255>.
34. «Сбер Банк представил технологию противодействия телефонному мошенничеству» // Банки.ру. URL: <https://www.banki.ru/news/lenta/?id=10953932> (дата обращения: 06.01.2025).
35. Признаки осуществления перевода денежных средств без согласия клиента: утв. приказом Банка России от 27 сентября 2018 года № ОД-2525. URL: https://cbr.ru/Content/Document/File/47786/priznaki_20180928.pdf (дата обращения: 06.01.2025).

REFERENCES

1. Decision of the Court of cassation dated 05.08.2014 in civil case No. ԵԿԴ/0426/02/13.
2. The Law of the Republic of Armenia “On Payment and Settlement Systems and Payment and Settlement Organizations” dated November 24, 2004 (with the latest amendments as of June 9, 2022) (clause “zha”, clause “e” of Art. 3).
3. Ibid.

4. Regulation of the Board of the Central Bank of the Republic of Armenia No. 300-N “On the procedure for establishing security rules aimed at protecting the interests of cardholders in connection with the issue, servicing and distribution of payment cards, as well as the implementation of transactions using payment cards in the territory of the RA” dated November 4, 2014 (with the latest amendments as of July 26, 2022) (clause 5).
5. Decision of the Board of the Central Bank of the Republic of Armenia No. 102-N “On approval of Regulation 4 “Minimum requirements for the implementation of internal control over banks” and cancellation of the decision of the Board of the Central Bank of the Republic of Armenia No. 71-N of March 11, 2008 dated April 18, 2013 (with the latest amendments as of October 14, 2024).
6. Decision of the Court of Cassation dated 07.04.2018 in the case of “Armenian Programs” LLC vs. Gagik Hovhannisyann, civil case No. ԵԱԳԳ/3614/02/15.
7. Decision of the Board of the Central Bank of the Republic of Armenia No. 102-N “On approval of Regulation 4 “Minimum requirements for the implementation of internal control over banks” and cancellation of the decision of the Board of the Central Bank of the Republic of Armenia No. 71-N of March 11, 2008 dated April 18, 2013 (with the latest amendments as of October 14, 2024).
8. Federal Law “On the National Payment System” of June 27, 2011 No. 161-FZ (with the latest amendments of August 8, 2024) (Articles 11–15).
9. Ibid.
10. Regulation of the Board of the Central Bank of the Republic of Armenia No. 300-N “On the procedure for establishing security rules aimed at protecting the interests of cardholders in connection with the issue, servicing and distribution of payment cards, as well as the implementation of transactions using payment cards in the territory of the RA” dated November 4, 2014 (with the latest amendments as of July 26, 2022) (clause 5).
11. Resolution of the Plenum of the Supreme Court of the Russian Federation of June 28, 2012 No. 17 “On the consideration by courts of civil cases on disputes regarding the protection of consumer rights” // “Rossiyskaya Gazeta”. No. 156. 2012.
12. *Karapetov A., Baibak V., Ivanov O., Lyubimova M., Makhalin I., Pavlov A., Sarbash S., Yastrzhembsky I.* Loan, credit, factoring, deposit and account: Article-by-article commentary to Articles 807–860.15 of the Civil Code of the Russian Federation Moscow: Logos, 2019. P. 1027.
13. Definition of the Supreme Court of the Russian Federation of January 17, 2023 No. 5-KG-22-121-K2. URL: https://www.vsrp.ru/stor_pdf.php?id=2211722 (accessed: 06.01.2025).
14. Definition of the Judicial Collegium for Civil Cases of the Supreme Court of the Russian Federation dated 16.12.2022 No. 5-KG22-127-K2 // Laws, codes and regulations of the Russian Federation. URL: <https://legalacts.ru/sud/opredelenie-sudebnoi-kollegii-po-grazhdanskim-delamverkhovnogo-suda-rossiiskoi-federatsii-ot-16122022-n5-kg22-127-k2/> (accessed: 06.01.2025).
15. On the refusal to accept for consideration the complaint of citizen Ksenia Andreevna Yushkova regarding the violation of her constitutional rights by paragraph 2 of Article 179 of the Civil Code of the Russian Federation: Determination of the Constitutional Court of the Russian Federation of 13.10.2022 No. 2669-O // Laws, codes and regulations of the Russian Federation: [website]. URL: <https://legalacts.ru/sud/opredelenie-konstitutsionnogo-suda-rfot-13102022-n-2669-o/> (accessed: 06.01.2025).

16. International Bank for Commerce and Development AD and Others v. Bulgaria, no. 7031/05, § 123, 2 June 2016, and BENet Praha, spol. s r.o. v. the Czech Republic, no. 33908/04, §§ 92-93, 24 February 2011, Yunusova and Yunusov v. Azerbaijan, no. 68817/14, § 167, 16.07.2020. URL: <https://hudoc.echr.coe.int/eng?i=001-203562>
17. The decision of the Constitutional Court of June 12, 2018 No. УԴՈ-1418 based on the application of Armine Atoyan, Hayk Nazinyan and Arkady Vardanyan on the conformity of Part 2 of Article 887 of the Civil Code of the Republic of Armenia with the Constitution of the Republic of Armenia. (clause 4.5).
18. *Braginsky M., Vitryansky V.* Contract Law. Book Five. In two volumes. Volume 2: Agreements on Bank Deposit, Bank Account; Bank Settlements. Competition, Agreements on Games and Betting. Moscow: Statut, 2006, p. 273; Russian Civil Law. Textbook. In 2 volumes. Vol. II: Law of Obligations / Ed. E.A. Sukhanov. 4th ed., stereotype. Moscow: Statut, 2015. P. 945; Civil Law of the Republic of Armenia. Part II. 2nd ed., with amendments and additions / T. Barseghyan, A. Aikyants, G. Garakhanyan, S. Megryan. Yerev.: Yerevan State University Publishing House, 2008. P. 430.
19. Protocol No. 1 to the European Convention for the Protection of Human Rights and Fundamental Freedoms of 20 March 1952. URL: <https://docs.cntd.ru/document/901867999> (accessed: 04 January 2025).
20. International Bank for Commerce and Development AD and Others v. Bulgaria, no. 7031/05, § 123, 2 June 2016, and BENet Praha, spol. s r.o. v. the Czech Republic, no. 33908/04, §§ 92-93, 24 February 2011, Yunusova and Yunusov v. Azerbaijan, No. 68817/14, § 167, 16.07.2020 Доступно по ссылке: <https://hudoc.echr.coe.int/eng?i=001-203562>
21. The decision of the Constitutional Court of June 12, 2018 No. УԴՈ-1418 based on the application of Armine Atoyan, Hayk Nazinyan and Arkady Vardanyan on the conformity of Part 2 of Article 887 of the Civil Code of the Republic of Armenia with the Constitution of the Republic of Armenia. (clause 4.5).
22. Ibid.
23. *Braginsky M., Vitryansky V.* Contract Law. Book Five. In two volumes. Volume 2: Agreements on Bank Deposit, Bank Account; Bank Settlements. Competition, Agreements on Games and Betting. Moscow: Statut, 2006, p. 273; Russian Civil Law. Textbook. In 2 volumes. Vol. II: Law of Obligations / Ed. E.A. Sukhanov. 4th ed., stereotype. Moscow: Statut, 2015. P. 945; Civil Law of the Republic of Armenia. Part II. 2nd ed., with amendments and additions / T. Barseghyan, A. Aikyants, G. Garakhanyan, S. Megryan. Yerevan: Yerevan State University Publishing House, 2008. P. 430.
24. The decision of the Constitutional Court of June 12, 2018 No. УԴՈ-1418 based on the application of Armine Atoyan, Hayk Nazinyan and Arkady Vardanyan on the conformity of Part 2 of Article 887 of the Civil Code of the Republic of Armenia with the Constitution of the Republic of Armenia. (clause 4.5).
25. “Ardshinbank” CJSC: General Terms. URL: <https://website-api.ardshinbank.am/files/documents/general-terms-arm-72b55f9a-483c-4076-83f4-cb270a9f2ef5.pdf> (accessed: 04.01.2025).
26. “ACBA BANK” OJSC Payment Card Issuance and Service Terms: URL: https://www.acba.am/files/eFO%2075-02-37.30_27.07.23.pdf (accessed: 04.01.2025).
27. Terms and conditions of service and rules of use of payment cards of “Ameriabank” CJSC. URL: https://ameriabank.am/Portals/0/files/announcements/green/Cards_terms_and_conditions_23_arm.pdf (accessed: 04.01.2025).

28. Terms and conditions of services provided to individuals by VTB Bank Armenia CJSC (public offer): URL: https://www.vtb.am/img/content/main-cards/OFERTA_arm_08-02.pdf (accessed: 04.01.2025).
29. General rules for opening and servicing (management) of bank and deposit accounts of “Fast Bank” OJSC. URL: fcstaticimages.blob.core.windows.net/fbfiles/account-type/1/Բանկային_և_ավանդային_հաշիվների_բացման_և_վարման_կանոններ.pdf (accessed: 04.01.2025).
30. The decision of the Constitutional Court of June 12, 2018 No. ՄԳՈ-1418 based on the application of Armine Atoyán, Hayk Nazinyan and Arkady Vardanyan on the conformity of Part 2 of Article 887 of the Civil Code of the Republic of Armenia with the Constitution of the Republic of Armenia. (clause 4.5).
31. Federal Law of the Russian Federation “On Amendments to Certain Legislative Acts of the Russian Federation” No. 340-FZ dated July 24, 2023. URL: <http://publication.pravo.gov.ru/document/0001202307240024?index=1> (accessed: 05.01.2025).
32. “Online exchange of information on fraudulent transactions will begin between the Bank of Russia and the Ministry of Internal Affairs of Russia” // Bank of Russia website. URL: <https://www.cbr.ru/press/event/?id=17142> (accessed: 05.01.2025).
33. *Repetskaya A., Petryakova L.* Victimological characteristics of fraud in the banking sphere (based on the materials from Siberian Federal District) // Russian Journal of Criminology. 2022. Vol. 16, No. 4. PP. 452-462. URL: <https://doi.org/10.17150/2500-4255>. (In Russ.).
34. Sberbank presented a technology to combat telephone fraud // Banki.ru. URL: <https://www.banki.ru/news/lenta/?id=10953932> (accessed: 06.01.2025).
35. Signs of a money transfer without the client’s consent: approved by Bank of Russia Order No. OD-2525 dated September 27, 2018. URL: https://cbr.ru/Content/Document/File/47786/priznaki_20180928.pdf (accessed: 06.01.2025).

FRAUD IN CASHLESS PAYMENTS: CIVIL-LAW ISSUES AND WAYS OF RESOLUTION

R. Amirova

Russian-Armenian University

ABSTRACT

The article explores the legal regulation of bank cards as a key tool for cashless payments and analyzes the legal implications of fraudulent activities involving their use. Special attention is given to the distribution of liability for losses arising from actions of cardholders, particularly in cases where they provide third parties with access to their cards, as well as the legal risks of adverse consequences resulting from such actions. The study examines the possibility of recovering funds by banks upon detecting signs of fraud and the legality of debiting funds from clients' accounts without their consent. The author concludes that certain provisions in agreements between banks and clients fail to comply with national legislation, potentially undermining the protection of property rights. Measures to improve the legal framework are proposed to enhance the security of bank card transactions and protect clients' interests.

Keywords: personal data protection, fraudulent transactions, cashless payments, property rights, notification.