№ исх: 29-2-02/1071 от: 25.12.2017
№ вх: 7396/ДЗ-288 от: 28.12.2017

«ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҰЛТТЫҚ БАНКІ»

РЕСПУБЛИКАЛЫҚ
МЕМЛЕКЕТТІК МЕКЕМЕСІ

050040, Алматы қ., Көктем-3, 21-үй
тел.: +7 727 2704591, факс: +7 727 2704655
телекс: 251130 BNK KZ, E-mail: hq@nationalbank.kz

РЕСПУБЛИКАНСКОЕ
ГОСУДАРСТВЕННОЕ УЧРЕЖДЕНИЕ

«НАЦИОНАЛЬНЫЙ БАНК РЕСПУБЛИКИ КАЗАХСТАН»

050040, г. Алматы, Коктем-3, дом 21
тел.: +7 727 2704591, факс: +7 727 2704655
телекс: 251130 BNK KZ, E-mail: hq@nationalbank.kz

25.12.2017ж. №29-2-02/1071

Қазақстан Республикасы Парламенті Мәжілісінің депутаттары

Ш.Х. Хахазовқа
В.К. Божкоға
Н.В. Жұмаділдаеваға
Р.У. КимгеН.Г. МикаелянғаА.С. МурадовқаШ.У. НурумовқаЮ.Е. ТимощенкоғаС.Ә. ҮмбетовкеМ.В. ЧирковқаП.А. Шарапаевқа

2017 жылғы 30 қарашадағы
№ДС-288депутаттық сауалға

Құрметті депутаттар!

Қазақстан Республикасының Ұлттық Банкі Сіздердің төлем карточкаларының иелерін алаяқтық әрекеттерден қорғау мақсатында банктер қабылдайтын шараларға қатысты сауалдарыңызды қарап, төмендегіні хабарлайды.

Төлем карточкаларын пайдалана отырып жүргізілетін алаяқтық тәуекелдердің алдын алу және барынша азайту, карточкаларды ұстаушыларды қорғау мәселелері қазіргі уақытта ең өзекті мәселелердің бірі болып табылады. Аталған мәселелерге қаржы реттеушісінің бақылау-қадағалау функцияларын жүзеге асыру және қаржылық қызметтерді тұтынушылардың құқықтарын қорғау шеңберінде Қазақстан Республикасының Ұлттық Банкі, сондай-ақ төлем карточкаларын шығару және олар пайдаланылатын операцияларға қызмет көрсету жөніндегі қызметтерді көрсететін тікелей нарық субъектілері – банктер мен халықаралық карточкалық төлем жүйелері (VISA, MasterCard және басқалары) айтарлықтай көңіл бөлуде.

Қазіргі уақытта практикада банктер төлем карточкаларын шет елде және алаяқтық тәуекелінің деңгейі жоғары елдерде пайдаланып та

жүргізілетін алаяқтық операциялардың алдын алудың/ескертудің қажетті әдістерін қолдануда:

- клиенттердің карточкалық операцияларына тәулік бойы мониторинг жүзеге асырылады, ықтимал алаяқтық схемалардың алдын алуға/болжауға, кибер-шабуылдарды анықтауға және алдын алуға бағытталған мамандандырылған бағдармалық қамтамасыз ету қолданылуда. Клиент үшін әдеттегідей емес операцияларды не заңсыз транзакцияны ықтимал жүргізуге өзге де күмән анықталған жағдайда, клиентпен тиісті жұмыс жүргізіледі, оның ішінде операция уақытша бұғатталады, телефон арқылы клиенттің растауы алынады және басқа қимылдар;

- SMS-хабарлама бойынша сервистер пайдаланылады, ондай қызметтер арқылы клиенттер төлем карточкасын пайдалана отырып әрбір транзакцияны бақылай алады, клиенттің төлемдерді санкциялауының қосымша әдістері (бірреттікпаролі бар SMS-хабар, кодтың растауын енгізу) пайдаланылады;

- сауда және қызмет көрсету ұйымдарында жүргізілген операцияларға (POS-терминал) талдау жасалады. Күмәнді операциялар анықталған кезде сауда желісіндегі POS-терминал барлық жағдай анықталғанға дейін бұғатталады;

- банкоматтардыскиммингтен қорғау үшін банктер кезеңдік негізде банкоматтарға инспекциялау жүргізеді, картадағы деректерді оқуға мүмкіндік бермейтін арнайы құралдарды пайдаланады, пернетақтаға қорғаныш жапсырмалар, сондай-ақ бейне тіркеу жүйелері орнатылады;

- интернет арқылы жүргізілетін операцияларға шектеулер қойылады, қажет болған кезде осы шектеулерді клиент өзгерте алады;

- ақпарат қорғаудың және клиенттерді сәйкестендірудің заманауи бағдарламалық құралдары қолданылады (қорғалған байланыс арналары, криптографиялық шифрлау, интернет пен мобильдікбанкингті пайдаланған кезде логинжәне пароль).

Сонымен қатар, банктер клиенттерге қашықтан хабарлау негізінде қаржылық қызметтерді алу кезінде болатын ықтимал тәуекелдер туралы, карточка деректерінің жария етілуіне жол бермеу және клиенттер үшін ықтимал салдарлар туралы хабарлау бойынша қажетті жұмыс жүргізеді.

Клиенттер алаяқтық деңгейі жоғары елдерде операциялар жүргізген кезде банктер операциялардың сомалары бойынша шектеулер белгілеу (клиенттің нұсқауы бойынша осы шектеулер алып тасталуы мүмкін), жүргізілген операцияларды растау үшін клиентпен кері байланыс, клиент шетелден қайтып келгеннен кейін карточкаларды қайта шығару сияқты қосымша қорғаныш іс-әрекеттерін қолдануы мүмкін.

Халықаралық төлем жүйелері (Visa, MasterCard) тарапынан сондай-ақ қауіпсіздік шараларын сақтау жөніндегі талаптарды (стандарттарды) ұсынады, оларды барлық банк – жүйенің қатысушылары ғаламдық деңгейде, оның ішінде ақпараттық қауіпсіздік, байланыс арналары, криптография құралдары бойынша сақтауға міндетті.

Бұл ретте банктерде клиенттердің алаяқтық операциялар жөніндегі шағымдарын қарау бойынша рәсімдер Қазақстан Республикасы заңнамасының және төлем карточкалары жүйелері қағидаларының талаптарын ескере отырып қатаң реттелген.

«Төлемдер және төлем жүйелері туралы» Қазақстан Республикасының Заңында төлем карточкасын ұстаушылардың рұқсат етілмеген операцияны өтеу туралы өтініштерін қарау мерзімі (үшінші тұлғалардан ақпаратты алу не тексеру жүргізу арқылы қосымша зерделеу қажет болған жағдайда күнтізбелік 15 күн – Қазақстан Республикасы ішіндегі операциялар бойынша күнтізбелік 30 күн, шетелде жасалған операциялар бойынша күнтізбелік 60 күн) белгіленеді, сондай-ақ төлем карточкасының жоғалуы, төлем карточкасының рұқсатсыз пайдаланылуы туралы төлем карточкасын ұстаушының хабарламасын алғаннан кейін рұқсат етілмеген операциялар жасалған жағдайда, олар үшінбанктердің жауапкершілігі айқындалады. Рұқсат етілмеген операцияны өтеуден бас тартуы клиенттің төлем карточкасын пайдалану қағидаларын бұзуын не оның төлем карточкасын пайдалана отырып алаяқтық операцияларға қатысуын растайтын негіздер, белгілер немесе фактілер болған кезде жүзеге асырылады.

Сонымен қатар Қазақстан Республикасының қолданыстағы заңнамасында клиенттен төлем карточкасының жоғалуы, ұрлануы немесе рұқсатсыз пайдалануы туралы хабарлама алған кезде банктерге банкоматтарға бейнебақылау жүйелерін міндетті түрде орнату, банктің карточканы дереу оқшаулау талаптары көзделген.

Шетелде алаяқтық операциялар жүргізілген кезде банктер клиенттердің өтініштерін қарауды халықаралық төлем жүйелерінде және жалпы қабылданған әлемдік практикада белгіленген талаптар негізінде жүзеге асырады. Көрсетілген жағдайларда клиенттен өтініш алған кезде банктер халықаралық төлем жүйесіне сұрату жібереді, ол эквайер банкпен тиісті жұмыс жүргізеді және алаяқтық операция расталған жағдайда қаражатты өтеу мүмкіндігі туралы қазақстандық банкке қорытынды ұсынады.

Оған қоса, төлем карточкаларын ұстаушылар сондай-ақ банктердің іс-әрекетіне қатысты Ұлттық Банкке шағым жасайды. Әрбіршағым бойынша банктерден клиенттің (өтініш берушінің) өтінішіне қатысты түсініктемелер, сондай-ақ төлем карточкаларын пайдалана отырып алаяқтық операцияларды жүзеге асыру әрекеттерін ашатын құжаттарды және ақпаратты алу жолымен тексеру жүргізіледі.

Оған қоса, алаяқтық операциялар бойынша ақша сомасын өтеу туралы мәселені толық банктерге ғана жүктеуге болмайды. Практика көрсетіп отырғандай алаяқтық операциялар көбіне клиенттердің төлем карточкалары деректемелерінің (банктік сервистерге қолжетімділіклогиндері мен парольдері, төлем карточкаларының нөмірлері, CVV (төлем карточкасының сырт жағындағы үш мәнді код), PIN-кодтың, банктен алынатынSMS-хабарламалардағы растау кодтарыныңконфиденциалдылығын сақтау бойынша ұсынымдарды ескермеуі салдарынан туындайтындығын көрсетеді. Қазақстан Республикасының заңнамасына сәйкес құпия код (PIN-код,

интернет транзакциялар үшін3D Secure код) дұрыс енгізілген кездегі операциялар клиент рұқсат етілген деп танылатындығын атап өткен жөн, бұл жалпы қабылданған әлемдік практика болып табылады.

Сондай-ақ клиенттер төлем карточкасын жоғалтып алу туралы банктерді әрқашан уақтылы хабардар етпейді.

Банктердің шығыстарды толық өтеуін (өтемақы) көздейтін талаптарды енгізу Қазақстан Республикасының аумағында алаяқтық операциялардың жиілеп кетуіне (клиенттердің қауіпсіздік талаптарын сақтауларын және конфиденциалды деректерді қорғауын кері ынталандыру, клиенттің өзі қатысатын «достық алаяқтықтың» өсуі) әкеліп соғуы, сондай-ақ алаяқтық операциялар бойынша ақшаны қайтаруға шығыстар клиенттердің күнделікті транзакцияларына тарифтерді өсіру есебінен өтелетін банктер тарифтерінің өсуіне және халықаралық төлем жүйелеріне әсер еуі мүмкін. Басқа елдердің іс-тәжірибелерінің талдауын ескере отырып, әділдік қағидаттарын және төлемге қатысушылардың (банк, төлем карточкалары жүйесінің операторы, клиент) өзара жауапкершілігін сақтау мақсаттарында оларды жүргізу клиенттің кінәсінен болуы мүмкін операцияларды қоса алғанда, алаяқтық операциялар бойынша барлық шығыстарды банктерге ғана жүктеу мүмкін емес.

Сонымен бірге, төлем карточкасы клиенттің иелігіндегі, оның бақылауы мен жауапкершілігіндегі банктік шоттағы ақшаға қолжеткізу құралы екенін ескеру қажет.

Бұл ретте Ұлттық Банк Қазақстан эмитенттерінің төлем карточкаларын пайдалана отырып жүргізілетін алаяқтық ахуалын мұқият қадағалайды, банк қоғамдастығымен бірлесіп халықтың қаржылық сауаттылығын арттыру және қаржылық қызметтерді тұтынушылардың құқықтарын қорғауды қамтамасыз ету жөніндегі қажетті іс-шаралар жүргізуде. Рұқсат етілмеген алаяқтық операциялардан қорғайтын жүйелі шараларды жетілдіру аясында ақпараттық қауіпсіздікті бұзу жағдайлары бойынша банктер арасында ақпарат алмасу жүйесін құру, банктердің карточкалық операцияларға мониторингті күшейтуі, алаяқтық іс-әрекеттерге ден қоюдың ішкі стандарттарын жақсарту бойынша, сондай-ақ алаяқтыққа қарсы тиімді іс-қимыл үшін халықаралық төлем жүйелерімен өзара байланысуды кеңейту бойынша мәселелер пысықталатын болады.

Төраға **Д. Ақышев**

Орынд. А.А.Нұрбаев, Р.А. Әбдірашев
Тел. +7 727 2704 800, +7 727 2704-591, ішкі 1-404

«ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҰЛТТЫҚ БАНКІ»

РЕСПУБЛИКАЛЫҚ
МЕМЛЕКЕТТІК МЕКЕМЕСІ

050040, Алматы қ., Көктем-3, 21-үй
тел.: +7 727 2704591, факс: +7 727 2704655
телекс: 251130 BNK KZ, E-mail: hq@nationalbank.kz

РЕСПУБЛИКАНСКОЕ
ГОСУДАРСТВЕННОЕ УЧРЕЖДЕНИЕ

**«НАЦИОНАЛЬНЫЙ БАНК
РЕСПУБЛИКИ КАЗАХСТАН»**

050040, г. Алматы, Коктем-3, дом 21
тел.: +7 727 2704591, факс: +7 727 2704655
телекс: 251130 BNK KZ, E-mail: hq@nationalbank.kz

25.12.2017г. №29-2-02/1071

**Депутатам
Мажилиса Парламента
Республики Казахстан**

**ХахазовуШ.Х.
БожкоВ.К.
Жумадильдаевой Н.В.
КимР.У.
МикаелянН.Г.МурадовуА.С.НурумовуШ.У.
Тимощенко Ю.Е.Умбетову
С.А.ЧирковуМ.В.ШарапаевуП.А.**

*На депутатский запрос
№ДЗ-288от 30 ноября 2017 года*

Уважаемые Депутаты!

Национальный Банк Республики Казахстан, рассмотрев Ваш запрос касательно мер, предпринимаемых банками в целях защиты владельцев платежных карточек от мошеннических действий, сообщает следующее.

Вопросы предупреждения и минимизации рисков мошенничества с использованием платежных карточек, защиты держателей карточек являются одними из наиболее актуальных в настоящее время. Указанным вопросам уделяется значительное внимание Национальным Банком Республики Казахстан в рамках осуществления контрольно-надзорных функций финансового регулятора и защиты прав потребителей финансовых услуг, а также непосредственно субъектами рынка, предоставляющими услуги по выпуску и обслуживанию операций с использованием платежных карточек – банками и международными карточными платежными системами (VISA, MasterCard и другие).

В настоящее время на практике банками применяются необходимые методы предотвращения/предупреждения мошеннических операций, в том числе при использовании платежных карточек за рубежом и в странах с повышенным уровнем риска мошенничества:

- осуществляется круглосуточный мониторинг карточных операций клиентов, применяются специализированные программные обеспечения, направленные на предупреждение/прогнозирование возможных мошеннических схем, обнаружение и предотвращение кибер-атак. При выявлении нетипичных для клиента операций либо иных подозрениях на возможное проведение несанкционированной транзакции банками проводится соответствующая работа с клиентом, в том числе, временное блокирование операции, получение от клиента подтверждения по телефону и другие действия;

- используются сервисы по SMS-уведомлению, посредством которых клиенты могут контролировать каждую транзакцию с использованием платежной карточки, применяются дополнительные методы санкционирования клиентом платежей (SMS-сообщение с одноразовым паролем, ввод кодового подтверждения);

- проводится анализ совершаемых операций в организациях торговли и услуг (POS-терминал). При выявлении сомнительных операций POS-терминал в торговой сети блокируется до выяснения всех обстоятельств;

- для защиты банкоматов от скимминга банки на периодичной основе осуществляют инспектирование банкоматов, используют специальные устройства, не позволяющие считать данные с карты, устанавливаются защитные накладки на клавиатуру, а также системы видеофиксации;

- устанавливаются ограничения на суммы операций, совершаемых посредством интернет, при необходимости данные ограничения могут быть изменены клиентом;

- применяются современные программные средства защиты информации и идентификации клиентов (защищенные каналы связи, криптографическое шифрование, логин и пароль при использовании интернет и мобильного банкинга).

Кроме того, банками проводятся необходимые работы по информированию клиентов о возможных рисках при получении финансовых услуг на дистанционной основе, о недопущении разглашения карточных данных и возможных последствиях для клиентов.

При проведении клиентами операций в странах с высоким уровнем мошенничества банками могут применяться дополнительные защитные действия, такие как установление ограничений по суммам операций (по указанию клиента данные ограничения могут быть сняты), обратная связь с клиентом для подтверждения совершаемых операций, перевыпуск карточек после возвращения клиента из-за рубежа.

Со стороны международных платежных систем (Visa, MasterCard) также выдвигаются требования (стандарты) по соблюдению мер безопасности, которые обязательны для соблюдения всеми банками – участниками систем на глобальном уровне, в том числе, по информационной безопасности, каналам связи, средствам криптографии.

При этом в банках строго регламентированы процедуры по рассмотрению обращений клиентов с жалобами на мошеннические операции

с учетом требований законодательства Республики Казахстан и правил систем платежных карточек.

Законом Республики Казахстан «О платежах и платежных системах» установлены сроки рассмотрения заявлений держателей платежных карточек о возмещении несанкционированной операции (15 календарных дней, при необходимости получения информации от третьих лиц или проведения проверки – 30 календарных дней по операциям, совершенным в Казахстане, 60 календарных дней по операциям, совершенным за рубежом), а также определена ответственность банков за несанкционированные операции в случае их совершения после получения уведомления держателя платежной карточки об утере карточки, несанкционированном использовании карточки. Отказ банком в возмещении несанкционированной операции осуществляется при наличии оснований, признаков или фактов, подтверждающих нарушение клиентом правил использования платежной карточки либо его участие в мошеннических операциях с использованием его платежной карточки.

Также действующим законодательством Республики Казахстан предусмотрены требования к банкам по обязательной установке систем видеонаблюдения на банкоматах, незамедлительному блокированию карточек банком при получении уведомления от клиента об утере, краже или несанкционированном использовании платежной карточки.

При проведении мошеннической операции за рубежом рассмотрение заявлений клиентов банками осуществляется на основании требований, установленных международными платежными системами и общепринятой мировой практикой. В указанных случаях при получении от клиента заявления банки направляют запрос в международную платежную систему, которая проводит соответствующую работу с банком-эквайером и представляет заключение казахстанскому банку о возможности возмещения средств в случае подтверждения мошеннической операции.

Кроме того, держатели платежных карточек также обращаются с жалобами на действия банков в Национальный Банк Республики Казахстана. По каждой жалобе проводится проверка путем получения от банков разъяснений по обращению клиента (заявителя), а также документов и информации, раскрывающих детали осуществления мошеннической операции с использованием платежной карточки.

Вместе с тем, вопрос о возмещении сумм денег по мошенническим операциям нельзя в полной степени возложить только на банки. Как показывает практика, мошеннические операции возникают в большинстве случаев вследствие пренебрежения клиентами рекомендаций по соблюдению конфиденциальности реквизитов платежной карточки (логины и пароли доступа к банковским сервисам, номера платежных карточек, CVV (трехзначный код на обратной стороне платежной карточки),PIN-кода, кодов подтверждений, получаемых от банка в SMS-сообщениях.Следует отметить, что в соответствии с законодательством Республики Казахстан операция при корректно введенном секретном коде (PIN-кода, код 3DSecuredляинтернет

транзакций) признается санкционированной клиентом, что является общепринятой мировой практикой.

Также не всегда клиенты своевременно уведомляют банки об утере платежной карточки, что может привести к потере средств клиентами.

Введение условий, предполагающих полное возмещение (компенсацию) расходов банками, может вызвать активизацию мошеннических операций на территории Республики Казахстан (дестимуляция клиентов к соблюдению требований безопасности и сохранности конфиденциальных данных, рост «дружеского мошенничества», в котором задействован сам клиент), а также может отразиться на увеличении тарифов банков и международных платежных систем, когда расходы на возврат денег по мошенническим операциям будут покрываться за счет увеличения тарифов по обычным клиентским транзакциям. С учетом анализа практики других стран, в целях соблюдения принципа справедливости и взаимной ответственности участников платежа (банк, оператор системы платежных карточек, клиент) не представляется возможным возложение всех расходов по мошенническим операциям только на банки, включая операции, совершение которых стало возможным по вине клиентов.

Вместе с тем, следует принять во внимание, что платежная карточка представляет собой инструмент доступа к деньгам на банковском счете, находящийся во владении у клиента, под его контролем и ответственностью.

При этом Национальный Банк внимательно отслеживает ситуацию по мошенничеству с использованием платежных карточек казахстанских эмитентов, совместно с банковским сообществом проводятся необходимые мероприятия по повышению финансовой грамотности населения и обеспечению защиты прав потребителей финансовых услуг. В рамках совершенствования защитных системных мер от несанкционированных мошеннических операций будут проработаны вопросы по созданию систем обмена информацией между банками по инцидентам нарушения информационной безопасности, усилению банками мониторинга за карточными операциями, улучшению внутренних стандартов реагирования на мошеннические действия, а также расширению взаимодействия с международными платежными системами для эффективного противодействия мошенничеству.

Председатель **Д. Акишев**

Исп. Нурбаев А.А., Абдрашев Р.А.
Тел. +7 727 2704 800,+7 727 2704-591, вн.1-404