Порядок использования кредитных банковских платежных карточек

Настоящий Порядок использования кредитных банковских платежных карточек (далее - Порядок) является неотъемлемой частью кредитного договора на потребительские нужды с использованием кредитной карточки, заключенного между ОАО «Белагропромбанк» (далее - Кредитодатель) и физическим лицом (далее - Кредитополучатель), определяет для Кредитодателя и Кредитополучателя порядок осуществления Кредитополучателем платежных операций (действия или совокупность действий, обеспечивающих осуществление платежа) с использованием платежного инструмента – личной кредитной банковской платежной карточки (использованием ее реквизитов). Порядок размещен на официальном сайте Кредитодателя в глобальной компьютерной сети Интернет по адресу: www.belapb.by (далее – сайт Кредитодателя).

1. ТЕРМИНЫ, ИСПОЛЬЗУЕМЫЕ В НАСТОЯЩЕМ ПОРЯДКЕ И ИХ ОПРЕДЕЛЕНИЯ

1.1. Авторизация - предоставление Кредитополучателю - держателю личной кредитной банковской платежной карточки (далее – карточка) права на ее использование, включая осуществление платежных операций с ее использованием, а также процесс проверки (подтверждения) таких прав при попытке использования карточки, включая осуществление платежных операций с ее использованием. Проверка (подтверждение) предоставленных прав при попытке использования карточки, включая осуществление платежных операций с ее использованием, не осуществляется в случаях, предусмотренных правилами платежной системы.

1.2. Аутентификация Кредитополучателя - процедура проверки предоставленных аутентификационных данных, предоставленных Кредитополучателем путем их сравнения с ранее зафиксированными Кредитодателем, банком-эквайером, иным уполномоченным лицом аутентификационными данными в целях подтверждения подлинности и принадлежности Кредитополучателю предоставленных аутентификационных данных.

1.3. Активация карточки – процедура снятия (отмены), установленного Кредитодателем в целях безопасности при выпуске карточки технического ограничения ее использования.

1.4. Жесткий стоп-лист - список карточек, запрещенных Кредитодателем к использованию, без возможности изъятия карточек из данного списка.

1.5. Компрометация карточки - наличие информации либо подозрения у Кредитодателя или иного поставщика платежных услуг, Кредитополучателя, иного лица об утере, хищении, незаконном присвоении, несанкционированном использовании карточки или реквизитов карточки, иных действиях, не санкционированных Кредитополучателем, позволяющих лицу, не являющемуся Кредитополучателем, незаконно использовать карточку или реквизиты карточки.

1.6. Карт-чек - информация, зафиксированная в электронном виде, включающая определенные реквизиты, позволяющие идентифицировать эту информацию, как относящуюся к карт-чеку, и подтверждающая успешное (неуспешное) завершение осуществленной с использованием карточки платежной операции инициирования платежа, операции выдачи наличных денежных средств.

1.7. ОТС - организация торговли (сервиса);

1.8. ПИН-код – персональный идентификационный номер, используемый Кредитодателем при проведении аутентификации Кредитополучателя.

1.9. 3D-Secure - дополнительная технология аутентификации при совершении операции оплаты товаров, работ и услуг в глобальной компьютерной сети Интернет при использовании карточек, на базе которой международными платежными системами разработаны специальные программы - Verified by VISA и Mastercard SecureCode,

национальной платежной системой Белкарт разработана технология - Белкарт-ИнтернетПароль, также платежной системой «Мир» разработана технология MirAccept.

1.10. CVC2/КПП2 - трехзначный код проверки подлинности карточки, который наносится на полосу для подписи и используется в качестве защитного элемента при проведении операций в глобальной компьютерной сети Интернет.

2. ПОРЯДОК АКТИВАЦИИ И ИСПОЛЬЗОВАНИЯ БАНКОВСКОЙ ПЛАТЕЖНОЙ КАРТОЧКИ

2.1. Карточка является собственностью Кредитодателя и по окончании срока ее действия должна быть возвращена в Кредитодателю.

Активация карточки осуществляется в момент генерации ПИН-кода с использованием технологии e-PIN, Кредитополучателем самостоятельно при совершении с использованием карточки следующих успешных операций, подтвержденных правильным вводом ПИН-кода: снятие наличных денежных средств; просмотр баланса (доступного остатка) по карточке; оплата товаров и услуг; смена ПИН-кода. Карточка не активируется в случае, если при проведении операции проверка ПИН-кода пройдена успешно, но сама операция отклонена (например, по причине недостаточности средств либо установления по карточке лимитов по проведению безналичных операций и (или) по получению наличных денежных средств); в случае неверного ввода ПИН-кода; нахождения карточки в стоп-листе (блокировки карточки).

Активация бесконтактного интерфейса карточки осуществляется после успешно проведенной финансовой операции по карточке с использованием контактного микропроцессора с вводом правильного ПИН-кода (выдача наличных денежных средств, оплата и др.) в банкомате (инфокиоске), расположенном на территории Республики Беларусь, или терминале, установленном у Кредитодателя или организации торговли (сервиса) на территории Республики Беларусь.

2.2. Пополнение карточки не осуществляется.

2.3. Карточка либо ее реквизиты не должны использоваться в противозаконных целях, включая покупку товаров (работ, услуг), запрещенных законодательством Республики Беларусь, а также законодательством государства, на территории которого используется карточка.

Подтверждением проведения операции, совершаемой с использованием карточки или ее реквизитов, являются карт чек и (или) иные документы (в т.ч. выписки по счету), предусмотренные правилами платежной системы и (или) локальными правовыми актами Кредитодателя. Карт чеки и иные документы, являющиеся подтверждением проведения операций, совершаемых при использовании карточки или ее реквизитов, могут составляться на бумажном носителе и (или) в электронном виде.

При совершении операций с применением карточки или ее реквизитов средствами аутентификации Кредитополучателя являются ПИН код, и (или) подпись Кредитополучателя на карт-чеке и (или) иные средства аутентификации Кредитополучателя. В случаях, предусмотренных правилами платежной системы, возможно совершение операций по карточке без авторизации.

Момент совершения операции, как правило, не совпадает с моментом отражения операции по Счету.

2.4. Совершение операций в банкоматах и других устройствах самообслуживания производится только с вводом ПИН-кода. Вводя ПИН-код Кредитополучатель признает правильность указанной в них суммы. При совершении операции допускается только три попытки неверного ввода ПИН-кода. При утрате ПИН-код не восстанавливается.

3. ИНФОРМАЦИОННО-КОНСУЛЬТАЦИОННАЯ ПОДДЕРЖКА

3.1. Контакт-центр Кредитодателя предоставляет следующую информацию по тел. 136:

вознаграждение за операции, совершенные при использовании карточек

Кредитодателя;

курсы валют, установленные для совершения валютно-обменных операций с использованием банковских платежных карточек Кредитодателя;

информационная поддержка в нестандартных ситуациях, возникающих при использовании карточки;

о местонахождении банкоматов, инфокиосков Кредитодателя.

3.2. Круглосуточная сервисная служба ОАО «Банковский процессинговый центр» (далее - служба сервиса (поддержки)) предоставляет следующие услуги:

внесение карточки в стоп-лист (блокировка) в случае ее утери, кражи, при подозрении на несанкционированное использование карточки или ее реквизитов по тел. +375 17 299 25 26;

изъятие карточки из стоп-листа, разблокировка карточки после превышения числа неверных попыток набора ПИН-кода, оказание консультаций информационно-справочного характера, управление жизненным циклом токена по тел. +375 17 299 25 25;

предоставление информации о доступной сумме по карточке по тел. +375 17 299 25 23.

4. СПОСОБЫ ПОЛУЧЕНИЯ ИНФОРМАЦИИ ОБ ОСУЩЕСТВЛЕННЫХ С ИСПОЛЬЗОВАНИЕМ КАРТОЧКИ ОПЕРАЦИЯХ

4.1. Информацию об осуществленных с использованием карточки операциях Кредитодатель предоставляет Кредитополучателю в виде выписки на бумажном носителе (выписка по счету) при личном обращении Кредитополучателя к Кредитодателю.

Дополнительно Кредитодатель предлагает следующие способы получения информации об осуществленных с использованием карточки операциях:

услуга «SMS-информирование» - позволяет получать посредством Push/SMS/Viber-сообщений информацию об операциях, совершенных при использовании карточки;

мини-выписка - формируемая Кредитополучателем самостоятельно в устройствах самообслуживания, системах «Интернет-банкинг», «Мобильный интернет-банкинг» выписка, содержащая информацию о последних авторизационных запросах по карточке (не более 13 запросов), исключая просмотр баланса, за определенное количество дней (не более 9);

выписка по счету в СДБО - формируемая Кредитополучателем самостоятельно в системах «Интернет-банкинг» и «Мобильный интернет-банкинг» выписка по счету.

4.2. В случае выявления неавторизованной операции Кредитополучатель обязан незамедлительно заблокировать карточку.

Датой получения Кредитополучателем информации об осуществленных с использованием карточки операциях в случае опротестования Кредитополучателем операции считается наиболее ранняя из следующих дат (определяется на основании сведений, зарегистрированных в информационных системах Кредитодателя или службе сервиса (поддержки), в зависимости от выбранного Кредитополучателем способа информирования):

дата направления Кредитодателем Кредитополучателю текстового сообщения на номер мобильного телефона в рамках подключенной Кредитополучателем услуги «SMS-информирование»;

дата получения Кредитополучателем мини-выписки в банкомате, инфокиоске, посредством систем «Интернет-банкинг», «Мобильный интернет-банкинг»;

дата получения Кредитополучателем выписки, формируемой самостоятельно в системах «Интернет-банкинг» и «Мобильный интернет-банкинг»;

дата получения Кредитополучателем выписки по счету на бумажном носителе при личном обращении к Кредитодателю (если Кредитополучатель не обращался за выпиской - первое число месяца, следующего за отчетным месяцем).

4.3. При выявлении несоответствия между отраженными в выписке и фактически осуществленными операциями Кредитополучатель имеет право требовать признания

совершенной платежной операции неавторизованной в случаях, определенных законодательством и Национальным банком Республики Беларусь.

Заявление о признании осуществленной с использованием карточки операции неавторизованной должно быть предоставлено Кредитополучателем на бумажном носителе Кредитодателю в течение одного месяца с даты выявления факта неавторизованной операции, но не позднее 70 календарных дней с даты отражения этой операции Кредитодателем.

Кредитодатель вправе устанавливать перечень документов, подлежащих предоставлению Кредитополучателем наряду с заявлением по неавторизованной операции в зависимости от характера оспариваемой операции, а также запрашивать дополнительные документы в процессе рассмотрения заявления или Кредитополучателя. Непредставление Кредитополучателем запрашиваемых Кредитодателем документов является основанием для отказа в проведении проверки.

Срок рассмотрения заявления о признании осуществленной с использованием карточного платежного инструмента операции неавторизованной исчисляется со дня, следующего за днем регистрации заявления у Кредитодателя. Если последний день срока рассмотрения заявления приходится на нерабочий день, то днем истечения срока считается первый следующий за ним рабочий день.

Кредитодатель информирует Кредитополучателя о результатах рассмотрения заявления о признании осуществленной с использованием карточного платежного инструмента операции неавторизованной в срок, не превышающий 90 календарных дней со дня регистрации заявления у Кредитодателя, путем направления Кредитополучателю уведомления на бумажном носителе или в электронном виде. Уведомление о результатах рассмотрения заявления помимо прочего включает в себя:

сведения о принятом Кредитодателем решении о признании (непризнании) осуществленной с использованием карточного платежного инструмента операции неавторизованной;

основания, установленные законодательством в области платежных систем и платежных услуг, для отказа в признании осуществленной с использованием карточного платежного инструмента операции неавторизованной (в случае принятия соответствующего решения);

конкретную дату исполнения решения о возмещении суммы неавторизованной операции (в случае принятия соответствующего решения);

сумму денежных средств, причитающихся Кредитополучателю в качестве возмещения.

4.4. Кредитополучатель вправе требовать признания операции неавторизованной, если осуществление этой операции стало возможным по причине компрометации карточного платежного инструмента в результате незаконного доступа к программно-техническим средствам банков, иностранных банков и (или) процессинговых центров и, как следствие, к реквизитам карточек и (или) информации, позволяющей несанкционированно использовать карточки.

Кредитополучатель предоставляют Кредитодателю заявление, содержащее требование о признании осуществленной с использованием карточки операции неавторизованной в соответствии с частью первой настоящего пункта, на бумажном носителе или в электронном виде. Подача такого заявления сроком не ограничивается.

При наличии у Кредитодателя информации о компрометации карточного платежного инструмента в случае, указанном в части первой настоящего пункта, заявление, содержащее требование о признании осуществленной с использованием карточного платежного инструмента операции неавторизованной, подлежит обязательному удовлетворению Кредитодателем в части операций, осуществленных с использованием скомпрометированной карточки, при условии соответствия заявленных Кредитополучателем реквизитов скомпрометированной карточки (аутентификационных данных) реквизитам (аутентификационным данным), имеющимся у Кредитодателя по

каждому конкретному случаю компрометации карточного платежного инструмента, и отсутствия у Кредитодателя информации о причастности Кредитополучателя к организации незаконного доступа к программно-техническим средствам банков, иностранных банков и (или) процессинговых центров.

В случае если Кредитополучателем по его инициативе была отменена блокировка скомпрометированного карточного платежного инструмента, осуществленная Кредитодателем в одностороннем порядке по причине компрометации карточного платежного инструмента в случае, указанном в части первой настоящего пункта, заявление, содержащее требование о признании осуществленной с использованием карточного платежного инструмента операции неавторизованной, подлежит удовлетворению в части операций, осуществленных с использованием скомпрометированного карточного платежного инструмента до момента инициированной Кредитополучателем отмены блокировки скомпрометированного карточного платежного инструмента.

В случае признания осуществленной с использованием карточки операции, указанной в части первой настоящего пункта, неавторизованной Кредитодатель не взимает вознаграждение (плату) за подачу и рассмотрение заявления, включая проведение всех необходимых процедур в соответствии с правилами платежной системы.

Возмещение суммы неавторизованной операции осуществляется путем инициирования платежа в безналичной форме Кредитодателем в пользу Кредитополучателя.

Возмещение суммы неавторизованной операции осуществляется без взимания Кредитодателем вознаграждения (платы) за осуществляемые в целях обеспечения возмещения необходимые процедуры, расчетные операции.

5. УТЕРЯ КАРТОЧКИ ИЛИ ПИН-КОДА, СМЕНА ПИН-КОДА, БЛОКИРОВКА КАРТОЧКИ

5.1. Если карточка утрачена, украдена, постороннему лицу стали известны реквизиты карточки и (или) ПИН-код либо при выявлении осуществленных с использованием карточки неавторизованных операций или ее реквизитов Кредитополучатель должен незамедлительно заблокировать карточку в службе сервиса (поддержки) по тел. +375 17 299 25 26(25), после чего уведомить Кредитодателя об этом в трехдневный срок для постановки карточки в жесткий стоп-лист путем предоставления заявления на бумажном носителе.

Карточка, которая передана или информация, о которой передана Кредитодателю третьими лицами, не являющимися клиентами (найденная карточка), подлежит обязательной блокировке работником Кредитодателя через службу сервиса (поддержки) по тел. +375 17 299 25 26.

5.2. Сменить ПИН-код карточки Кредитополучатель может, обратившись в любое Подразделение либо самостоятельно в СДБО. При этом ПИН-код будет направлен Кредитополучателю посредством SMS-сообщения при использовании технологии e-PIN.

Также Кредитополучатель, может сменить ПИН-код карточки в банкоматах Кредитодателя.

За смену ПИН-кода Кредитодатель взимает вознаграждение, установленное Сборником платы (вознаграждений) за операции, осуществляемые Кредитодателем.

5.3. Кредитополучатель, обязан предоставить по требованию Кредитодателя информацию для расследования обстоятельств утраты карточки. Если Кредитодатель имеет сведения о том, что незаконное использование карточки произошло с ведома Кредитополучателя, то ответственность за совершенные при использовании карточки операции несет Кредитополучатель.

При обнаружении карточки, ранее объявленной украденной или утерянной, использование такой карточки категорически запрещено.

5.4. Если карточка заблокирована по инициативе Кредитодателя или Кредитополучателя, по причине ее компрометации, то Кредитополучатель вправе требовать от Кредитодателя разблокировать карточку в целях возобновления возможности

ее использования. В случае поступления такого требования от Кредитополучателя, Кредитодатель разблокирует карточку.

6. ОСОБЕННОСТИ СОВЕРШЕНИЯ ВАЛЮТНО-ОБМЕННЫХ ОПЕРАЦИЙ

6.1. Кредитополучатель до проведения валютно-обменных операций выражает свое согласие на использование при их проведении обменных курсов, установленных Кредитодателем, следующими способами:

при совершении операции с использованием СДБО - посредством подтверждения совершения операции с использованием обменных курсов после ознакомления с ними;

при совершении операции в банкомате или инфокиоске Кредитодателя - посредством нажатия кнопки или выбора элемента интерфейса, которые инициируют совершение соответствующей операции;

при совершении иных операций:

если при совершении операции осуществляется аутентификация Кредитополучателя - посредством совершения действий для аутентификации Кредитополучателя;

если при совершении операции не осуществляется аутентификация Кредитополучателя - посредством совершения действий по инициированию совершения соответствующей операции.

В случае если валюта операции не совпадает с валютой счета, а также в некоторых случаях, предусмотренных платежными системами, проводится валютно-обменная операция. Валютно-обменные операции совершаются по курсам, установленным Кредитодателем на момент совершения операции, с учетом кросс-курсов платежной системы. Валютно-обменные курсы для проведения операций при использовании карточек могут быть изменены в течение рабочего дня в соответствии с ЛПА Кредитодателя, регламентирующим установление курсов валют по операциям с использованием карточек. Информация об установленных Кредитодателем курсах валют по операциям с карточками размещается на главной странице корпоративного сайта Кредитодателя, в системах дистанционного банковского обслуживания клиентов (Интернет-банкинг, мобильный банкинг), а также в подразделениях Кредитодателя в общедоступном для клиентов месте.

Информация о курсах валют, установленных платежными системами, размещается на сайте платежной системы.

Для операций, совершенных в устройствах банков, не подключенных к ОАО «Банковский процессинговый центр» (далее - БПЦ), момент совершения валютно-обменной операции определяется на основании расчетной информации, поступившей от платежной системы. В случае, когда платежная система в расчетной информации не указывает время совершения операции, для совершения такой операции применяют валютно-обменные курсы, установленные последним за эту дату распоряжением.

Для операций, совершенных в устройствах Кредитодателя или банков, подключенных к БПЦ, момент совершения валютно-обменной операции определяется исходя из даты и времени совершения операции.

По факту проведения Кредитополучателем валютно-обменной операции Кредитодатель формирует документ, подтверждающий проведение валютно-обменной операции. Документ формируется (выводится на печать или интерфейс устройства) с использованием устройства Кредитодателя, в котором Кредитополучателем проводится валютно-обменная операция. Данный документ содержит информацию, предусмотренную законодательством.

6.2. Обработка операций при использовании карточек производится в двух системах. Первоначально - в системе обработки авторизационных запросов, в которой в режиме реального времени изменяется доступная сумма по карточке, а затем - в системе клиринга, в которой формируется расчетная информация. Только по мере обработки Кредитодателем расчетной информации сумма операции отражается по счету Кредитополучателя.

Поскольку обменные курсы устанавливаются МПС ежедневно и обновляются с учетом ситуации на валютном рынке, сумма операции в валюте счета на этапе авторизации

и на этапе отражения операции по счету может отличаться (в меньшую или большую сторону).

7. ОСОБЕННОСТИ СОВЕРШЕНИЯ ОПЕРАЦИЙ В ГЛОБАЛЬНОЙ КОМПЬЮТЕРНОЙ СЕТИ ИНТЕРНЕТ

7.1. Кредитодатель предоставляет Кредитополучателю возможность совершения операций оплаты товаров, работ и услуг в глобальной компьютерной сети Интернет с применением реквизитов карточки с учетом следующих особенностей:

Кредитодатель предоставляет Кредитополучателю возможность использования технологий 3D-Secure;

для подтверждения совершения операции в глобальной компьютерной сети Интернет как правило используется CVC2/КПП2, однако при совершении повторных (подписанных) платежей в одной и той же ОТС допускается отсутствие подтверждения CVC2/КПП2.

Кредитодатель имеет право устанавливать ограничения на совершение операций оплаты товаров, работ и услуг в глобальной компьютерной сети Интернет (в том числе с применением технологии 3D-Secure) при использовании карточек.

7.2. Кредитополучатель несет ответственность за операции, совершенные с использованием карточки или ее реквизитов в глобальной компьютерной сети Интернет (далее - Интернет-платежи).

Кредитополучатель несет все риски, связанные с проведением Интернет-платежей и осуществлением иных действий, связанных с внесением и сохранением реквизитов карточки на Интернет-сайтах.

Кредитополучатель не может предъявлять Кредитодателю претензии по операциям, проведенным в глобальной компьютерной сети Интернет при использовании карточки, в случае нарушения настоящего Порядка.

Кредитодатель не несет ответственность в случае невозможности проведения Кредитополучателем Интернет-платежей по независящим от Кредитодателя обстоятельствам.

Введение правильных реквизитов карточки и/или проверочного кода 3D-Secure является надлежащей и достаточной аутентификацией Кредитополучателя для отражения по Счету операции, совершенной при использовании карточки и ее реквизитов.

7.3. Раскрытие информации в соответствии со статьей 23 Закона Республики Беларусь от 19.04.2022 № 164-З «О платежных системах и платежных услугах» производится Кредитодателем посредством размещения Правил платежной системы ОАО «Белагропромбанк» на официальном сайте Кредитодателя в глобальной компьютерной сети Интернет по адресу: www.belapb.by.

8. РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОМУ ИСПОЛЬЗОВАНИЮ КАРТОЧКИ

8.1. Сохраните номер телефона службы сервиса (поддержки) карточек Кредитодателя в легкодоступном месте (например, в памяти мобильного телефона или записной книжке), эта информация может пригодиться для блокировки карточки в случае ее утери либо кражи.

8.2. Обеспечивайте условия хранения карточки, которые исключают возможность ее утери, порчи, копирования данных, несанкционированного и незаконного использования. Не допускайте механических повреждений на карточке, деформации, загрязнения, воздействия высоких и низких температур, электромагнитных полей, прямых солнечных лучей, влаги, красителей, растворителей, вредных химических веществ и других неблагоприятных факторов, которые могут повлечь неработоспособность карточки.

8.3. Не передавайте карточку третьим лицам. Право пользования карточкой имеет только Кредитополучатель.

8.4. Храните в тайне от других лиц конфиденциальные данные карточки: номер и срок действия карточки, указанный на оборотной стороне трехзначный код проверки подлинности карточки (при его наличии), ПИН-код, который необходимо запомнить или, в случае если это является затруднительным, хранить его отдельно от карточки в неявном

виде (например, переписав его на листок бумаги среди прочих групп цифр или любой другой информации). Никогда не сообщайте ПИН-код другим лицам, включая родственников, знакомых, работников банков, ОТС, представителей правоохранительных органов. Не передавайте ПИН-код ни по телефону, ни по электронной почте. Только Кредитополучатель должен знать свой ПИН-код.

8.5. Настоятельно рекомендуем использовать услугу «SMS-информирование», которая обеспечивает оперативное получение информации о каждой осуществленной с использованием карточки операции, повлекшей изменение размера задолженности по Счету. При поступлении Push/SMS/Viber-сообщения об операции, которую Вы не совершали, необходимо незамедлительно заблокировать карточку и обратиться к Кредитодателю.

Если при наличии подключенной услуги «SMS-информирование» сообщения от Кредитодателя о проводимых операциях перестали поступать на Ваш мобильный телефон, необходимо связаться с Кредитодателем для уточнения причин, чтобы исключить возможность перехвата Push/SMS/Viber-сообщений третьими лицами. Если полученное Push/SMS/Viber-сообщение вызывает какие-либо сомнения или опасения, оперативно обратитесь к Кредитодателю для получения разъяснений.

8.6. Для взаимодействия с Кредитодателем используйте только реквизиты средств связи (мобильных и стационарных телефонов, факсов, Интернет-сайтов, обычной и электронной почты), которые указаны в документах, полученных непосредственно у Кредитодателя.

8.7. При утере, краже карточки, оставлении ее в банкомате или ином устройстве самообслуживания, изъятии кассиром ОТС, компрометации карточки (если конфиденциальные данные карточки стали известны посторонним лицам) либо при возникновении таких подозрений необходимо немедленно заблокировать карточку (например, позвонив в службу сервиса (поддержки), или посредством СДБО) и обратитесь к Кредитодателю.

8.8. Проведение операций при использовании карточки в банкоматах и инфокиосках.

При выборе банкомата или инфокиоска, в котором вы собираетесь провести операцию при использовании карточки, желательно избегать плохо освещенных и безлюдных мест. Наиболее безопасными местами для совершения операций являются помещения банковских офисов, уличные же банкоматы в туристических районах являются менее безопасными.

Для совершения регулярных операций старайтесь пользоваться одним и тем же банкоматом, расположенным в хорошо освещенном месте: вам будет проще выявить факт установки на него стороннего оборудования, которое может использоваться мошенниками для похищения информации с карточек.

Перед началом обслуживания осмотрите лицевую панель банкомата. Банкоматы некоторых банков предлагают сверить изображение банкомата на мониторе с тем, который перед вами. Обратите особое внимание на щель картоприемника: мошенники могут установить на него не предусмотренную конструкцией банкомата накладку. Перед использованием банкомата или другого устройства самообслуживания потрогайте панели, попробуйте их подвигать: фальшивые накладки и клавиатуры обычно держатся плохо и, как правило, даже при незначительном воздействии шатаются, отходят или даже отпадают. Зачастую мошенники оставляют заметные следы: щели, клеевые подтеки и сколы. Лучше не использовать банкомат, картоприемник которого выглядит так, будто кто-то ковырял его отверткой или облил клеем.

Порой мошенники делают поддельные панели с видеокамерами, которые затем крепятся к банкомату: на диспенсер для денег, под козырек, под экран или даже в стенде для рекламных брошюр. Эти камеры издалека могут выглядеть как черные точки.

Если клавиатура неестественно выпирает, шатается или отличается по тону, выглядит новой, в то время как сам банкомат уже имеет явные признаки изношенности, - это также повод отказаться от использования такого устройства самообслуживания.

8.9. Не применяйте чрезмерную физическую силу, чтобы вставить карточку в банкомат (инфокиоск). Если банковская карточка не вставляется без дополнительных усилий, воздержитесь от использования данного банкомата (инфокиоска).

В некоторых банкоматах (инфокиосках) могут применяться специальные устройства, которые препятствуют копированию мошенниками данных о карточках, - джиттеры. В таких банкоматах (инфокиосках) процесс приема карточек устройством может отличаться от других банкоматов (инфокиосков) - карточка вибрирует в момент ее приема устройством.

8.10. При обнаружении постороннего оборудования (например, накладки) не пытайтесь снять его самостоятельно, воздержитесь от совершения операций, а о выявленной накладке сообщите в банк, обслуживающий устройство. Если сомнения относительно корректной работы банкомата или другого устройства самообслуживания возникли после того, как карточка помещена в картоприемник, не вводите ПИН-код. Нажмите кнопку для отмены операции и заберите карточку. Если вы заметили постороннее оборудование уже после окончания обслуживания, обязательно сразу же заблокируйте карточку любым доступным способом.

Убедитесь, что выбранный вами банкомат или другое устройство самообслуживания принимает имеющуюся у вас карточку. Логотип на вашей карточке и на экране программно-технического устройства и (или) на его корпусе должны быть одинаковы. Если вы вставили в банкомат или другое устройство самообслуживания карточку, не обсуживающуюся в данном устройстве, карточка будет вам возвращена, при этом на экране появится информация о невозможности совершения операции.

В случае если поблизости от банкомата или другого устройства самообслуживания находятся люди, вызывающие у вас подозрение, следует выбрать другое время для использования данного устройства или воспользоваться другим банкоматом или устройством самообслуживания.

Будьте особенно осторожны, если незнакомые люди предлагают вам помощь в использовании карточки в банкомате или другом устройстве самообслуживания. В случае затруднений, возникших при использовании карточки, не прислушивайтесь к советам посторонних лиц, а для связи с Банком пользуйтесь только номерами телефонов, которые указаны непосредственно на карточке либо получены вами из надежных проверенных источников или непосредственно к Кредитодателю.

Обращайте внимание на людей, стоящих за вами в очереди у банкомата или другого устройства самообслуживания, в случае необходимости попросите их отойти на расстояние, с которого они не смогут увидеть вводимый вами ПИН-код. При вводе ПИН-кода находитесь как можно ближе к банкомату или устройству самообслуживания, при этом прикрывайте клавиатуру ладонью свободной руки.

При использовании карточки внимательно изучайте информацию, выводимую на экран банкомата или другого устройства самообслуживания, и проверяйте правильность вводимых данных. При неоднократном некорректном вводе ПИН-кода карточка блокируется и может быть изъята банкоматом или другим устройством самообслуживания. В случае изъятия карточки (независимо от причины) банкоматом или другим устройством самообслуживания немедленно заблокируйте ее (например, связавшись со службой сервиса (поддержки) или с использованием СДБО).

Не позволяйте никому отвлекать вас во время проведения операции, поскольку вы можете случайно совершить некорректную операцию. Кроме того, при отсутствии каких-либо действий с вашей стороны в течение установленного для данного устройства времени оно может изъять вашу карточку и (или) деньги.

После получения наличных денежных средств в банкомате следует убедиться в том, что карточка была возвращена банкоматом, дождаться выдачи карт-чека (при его запросе) и только после этого отходить от банкомата. Следует помнить, что последовательность выдачи наличных денежных средств и возврата карточки в банкоматах разных банков может отличаться. Банкомат может сначала вернуть карточку, а затем выдать запрошенную

сумму денежных средств. Необходимо учитывать данную специфику работы банкоматов и не отходить от устройства до момента получения карточки, карт-чека (при его запросе) и денег.

В случае если банкомат или другое устройство самообслуживания работает некорректно (например, долгое время находится в режиме ожидания, самопроизвольно перезагружается), следует отказаться от использования такого устройства, отменить совершаемую операцию, нажав на клавиатуре соответствующую кнопку, и дождаться возврата карточки. Если устройство не возвращает карточку, следует незамедлительно заблокировать карточку любым доступным способом и обратиться к Кредитодателю.

Не оставляйте запрошенный вами карт-чек в банкомате или другом устройстве самообслуживания, так как в чеке могут быть указаны сумма операции, остаток денежных средств. Это может привлечь грабителя или мошенника.

8.11. Получение наличных денежных средств и проведение операций безналичной оплаты при использовании карточки в подразделениях банков.

Все действия работника банка с карточкой должны проходить под вашим наблюдением. Не разрешайте работнику банка уходить с карточкой в другое помещение.

При получении наличных денежных средств либо проведении безналичной оплаты особое внимание обращайте на соответствие указанной суммы и суммы, содержащейся в карт-чеке (слипе).

При проведении операций в ПВН обращайте особое внимание на действия работника банка, если он пытается провести вашу карточку через считывающее устройство оборудования больше одного раза. Это позволит предотвратить проведение неавторизованных операций. Обязательно поинтересуйтесь причиной, по которой работнику необходимо повторно провести карточку через считывающее устройство оборудования.

Перед вводом ПИН-кода внимательно изучите информацию, представленную на экране терминала, а также убедитесь, что сумма и валюта операции верны.

Вводите ПИН-код, прикрывая клавиатуру ладонью свободной руки. Никогда и ни при каких обстоятельствах не сообщайте ПИН-код работникам банка.

Перед тем как подписать карт-чек, убедитесь, что сумма и валюта операции, дата операции, тип операции и другие данные, указанные в карт-чеке, верны.

8.12. Проведение операций безналичной оплаты при использовании карточки в ОТС.

Используйте карточки в ОТС, которые вызывают доверие.

При проведении операций в ресторанах, барах, магазинах, отдавая карточку обслуживающему персоналу, не выпускайте ее из поля зрения. При необходимости проследуйте за работником ОТС к терминалу. Это позволит предотвратить неправомерное копирование информации, указанной на карточке.

При совершении операции с использованием принтера или платежного терминала (POS-терминала) кассир может потребовать ввести ПИН-код или подписать карт-чек в соответствии с требованиями, установленными правилами платежной системы.

При проведении операции оплаты в ОТС обращайте особое внимание на действия кассира, если он пытается провести карточку через считывающее устройство оборудования больше одного раза. Это позволит предотвратить проведение несанкционированных операций. Обязательно поинтересуйтесь причиной, по которой кассиру необходимо повторно провести карточку через считывающее устройство оборудования. Если вследствие неуспешной операции по карточке вы оплатили покупку иным способом (например, наличными или иной карточкой), сохраните подтверждающий документ и проверьте, списались ли со счета денежные средства по неуспешной операции.

Вводите ПИН-код, прикрывая клавиатуру ладонью свободной руки. Перед набором ПИН-кода следует убедиться в том, что люди, находящиеся в непосредственной близости от Вас, не смогут его увидеть. Никогда и ни при каких обстоятельствах не сообщайте ПИН-код работникам ОТС.

Перед тем как подписать карт-чек, убедитесь, что сумма и валюта операции, номер

карточки (его часть), дата операции, тип операции, название ОТС и другие данные, указанные в карт-чеке, верны.

Если вы решили отказаться от покупки после успешного завершения операции, потребуйте отменить операцию. Обязательно сохраните карт-чек по операции отмены до сверки выписки по счету, к которому выпущена карточка.

Бесконтактные операции совершаются в режиме «самообслуживания»: Кредитополучатель не передает карточку или другой платежный инструмент, используемый для оплаты (например, браслет, брелок, мобильный телефонов или другое устройство) кассиру, а самостоятельно прикладывает карточку или другой платежный инструмент к считывающему устройству терминала для проведения операции.

8.13. Проведение операций безналичной оплаты при использовании карточки в глобальной компьютерной сети Интернет.

Для обеспечения наиболее высокого уровня безопасности операций подключите услугу подтверждения операций по технологии 3D-Secure. Данные технологии позволяют запросить дополнительное подтверждение операций, совершаемых в глобальной компьютерной сети Интернет, с помощью одноразового пароля, высылаемого на телефон (посредством Push/SMS/Viber-сообщения), указанный при подключении услуги.

Не отвечайте на электронные письма, в которых от имени якобы Кредитодателя или иных организаций, а также граждан просят предоставить персональную информацию, в том числе реквизиты карточки, в целях их обновления или для регистрации. Постарайтесь выяснить правомерность таких предложений, связавшись с Кредитодателем по достоверно известному номеру телефона (например, полученному вами непосредственно от Кредитодателя при получении карточки).

Передавайте информацию о своей карточке только для оплаты покупки. Никогда не пересылайте данные карточки по электронной почте, так как передаваемая по электронной почте информация не полностью защищена от перехвата и использования посторонними. На сайтах всех известных благонадежных магазинов используется технология шифрования данных, которая защищает Вашу информацию личного характера при совершении покупки.

Никогда не показывайте номер карточки в доказательство достижения Вами определенного возраста, хотя иногда на некоторых сайтах могут попросить это сделать. Номер карточки не может указывать на достижение Вами какого-либо возраста.

Злоумышленники часто распространяют вирусные программы через различные Интернет-ресурсы - от социальных сетей до обычных новостных сайтов. Кредитополучатель, компьютер которого заражен, при попытке войти в личный кабинет может быть незаметно перенаправлен на «фишинговый» сайт, который внешне практически не отличается от подлинных сайтов Интернет-банков, интернет-магазинов или других платежных сервисов. Чтобы этого избежать, старайтесь максимально использовать возможности вашего браузера и почтового клиента по обеспечению безопасности. Для этого в опциях браузера и почтового клиента необходимо включить дополнительные функции. Например, «Блокировка всплывающих окон», «Защита от фишинга и вредоносного ПО», «Открывать файлы на основе содержимого, а не расширения» и др. Также не стоит пользоваться окном предварительного просмотра в используемом вами почтовом клиенте.

Кроме того, рекомендуется всегда самостоятельно вводить веб-адрес банка («Интернет-банкинга») в адресную строку браузера вместо использования любых гиперссылок, тем более из подозрительных сообщений.

Делайте покупки в известных Вам интернет-магазинах или сначала убедитесь в том, что они пользуются хорошей репутацией и надежны. Проверяйте правильность адресов Интернет-сайтов, к которым подключаетесь для совершения покупки, так как похожие адреса могут использоваться для осуществления неправомерных действий. Если у вас появились какие-либо подозрения относительно Интернет-страницы или вы не хотите предоставлять персональные или карточные данные, то покиньте страницу и произведите покупку в другом месте.

Во время совершения оплаты по карточке в глобальной компьютерной сети Интернет удостоверьтесь, что фрагмент веб-адреса «http» в адресной строке веб-браузера изменился на «https» - это будет означать, что сессия зашифрована. Большинство браузеров дополнительно визуализируют такое изменение изображением навесного замка, кликнув по которому, можно просмотреть сертификаты, подтверждающие безопасность расчетов через данный сайт.

Перед совершением операции оплаты товара (услуги) внимательно изучите условия предлагаемого соглашения, в частности, все правила предоставления услуг, условия доставки, возврата, замены товара, а также процедуру отмены заказа. Особенно внимательно читайте условия совершения операций, связанных с азартными играми (казино, лотереи), так как они могут предусматривать автоматическую подписку, что повлечет списание денежных средств на регулярной основе. Отдельно оцените целесообразность совершения операции, если информация об условиях покупки изложена на незнакомом языке. Найдите номер телефона или адрес электронной почты ОТС и запишите их на случай, если у Вас возникнут вопросы.

Ведите учет операций, совершенных в глобальной компьютерной сети Интернет, включая адреса сайтов интернет-магазинов. Многие интернет-магазины посылают покупателям электронные сообщения с обобщающей информацией об операциях - сохраните или распечатайте их. Сохраняйте любые электронные документы, переписку по электронной почте, касающуюся попыток разрешения спорной ситуации с ОТС, так как данные документы могут оказаться очень важны для защиты ваших прав. При невозможности самостоятельно разрешить спорную ситуацию обратитесь к Кредитодателю.

Если было произведено бронирование гостиницы через Интернет-сайт, но по каким-то причинам не планируется воспользоваться ею, обязательно проведите отмену бронирования через тот же Интернет-сайт согласно указанным на нем процедурам. Получение Кредитополучателем кода отмены бронирования отеля является доказательством того, что бронь действительно отменена. В ином случае за несвоевременную отмену брони гостиница имеет право представить к списанию со счета сумму денежных средств в установленном ею размере.

Никогда не сообщайте свой ПИН-код при заказе товаров по телефону или почте и не вводите его нигде в Интернете. Для совершения подобных операций ПИН-код никогда не используется.

Убедитесь в том, что проводимые Вами операции соответствуют закону. Если на сайте интернет-казино или на других сайтах азартных игр присутствуют логотипы платежных систем, то это НЕ означает, что проведение операций, связанных с участием в азартных играх, правомерно. Если у Вас возникли какие-либо вопросы или сомнения в правомерности совершаемых операций, обратитесь к Кредитодателю.

Совершайте покупки только со своих устройств, не пользуйтесь Интернет-кафе и другими общедоступными средствами, где могут быть установлены программы-шпионы, запоминающие вводимые Вами конфиденциальные данные.

Устанавливайте на свои устройства лицензионное программное обеспечение, в том числе антивирусное, и межсетевые экраны (фаерволы/брандмауэры) и регулярно производите их обновление. Это поможет защитить ваши устройства от вирусов и других деструктивных программ, а также от несанкционированного доступа к вашим конфиденциальным данным. Даже если вы уверены в своем программном обеспечении, не стоит открывать или загружать вложения электронных писем от незнакомых и сомнительных адресатов.

Подключитесь к услугам Кредитодателя, позволяющим осуществлять оперативный контроль за расходами по карточке («Интернет-банкинг», «Мобильный интернет-банкинг», «SMS-информирование» и пр.).

При появлении подозрений о неправомерном списании денег рекомендуем незамедлительно осуществить блокировку карточки и обратиться к Кредитодателю.

8.14. Использование СДБО.

Храните в тайне от других лиц конфиденциальные данные карточки: номер и срок действия карточки, указанный на оборотной стороне трехзначный код проверки подлинности карточки (при его наличии), а также сведения, касающиеся учетных записей в СДБО: логины, пароли, коды доступа, данные из Push/SMS/Viber-сообщений и т.д.

При использовании системы «Интернет-банкинг» обращайте внимание на наличие на странице сервиса защищенного протокола HTTPS. Перед входом в систему рекомендуется удостовериться в подлинности сертификата и сайта. Как правило, для этого необходимо кликнуть в поле адресной строки Интернет (поле с пиктограммой замка или листа бумаги) и сверить имеющуюся в блоке информацию. В случае несоответствия присутствующих данных с реальными сведениями о Кредитодателе стоит немедленно покинуть страницу.

Не забывайте периодически (а также в случае, если пароль стал известен посторонним лицам) менять свой пароль. Старайтесь сделать его максимально сложным и уникальным. Для этого используйте в пароле прописные и строчные буквы, цифры и символы. Не используйте один и тот же пароль в разных системах (электронная почта, системы «Интернет-банкинг» других банков, социальные сети и т.п.). Постарайтесь избегать в пароле даты своего рождения, имени и других доступных о вас данных. Ни при каких обстоятельствах не разглашайте свой пароль никому, включая работников банка.

Будьте осторожны, посещая сайты с сомнительным содержанием: именно они, как правило, являются источником самых новых вирусов.

По окончании сеанса работы с системой «Интернет-банкинг» обязательно корректно выходите из системы, используя соответствующую опцию.

8.15. Проведение операций с использованием приложений и «Мобильный интернет-банкинг».

Устанавливайте мобильные приложения (в том числе и приложения Кредитодателя) только из известных источников (Google Play, Windows Store, App Store или AppGallery). Рекомендуется использовать антивирус для мобильных устройств.

Помните, что Кредитодатель не рассылает ссылки или указания на установку приложений через Push/SMS/Viber/MMS/e-mail-сообщения.

Не устанавливайте мобильные приложения Кредитодателя на мобильный телефон (устройство), на котором получены root-права (права суперпользователя). Такие телефоны и устройства также не рекомендуется использовать для получения сообщений от Кредитодателя (например, SMS с кодом (одноразовым паролем) для прохождения аутентификации).

При утрате мобильного телефона (устройства), на котором установлено мобильное приложение Кредитодателя (приходят Push/SMS/Viber-сообщения с подтверждающими одноразовыми паролями), или неожиданном прекращении работы SIM-карты следует как можно быстрей заблокировать SIM-карту.

8.16. Особенности проведения операций при использовании карточки.

Необходимо учитывать, что специфика совершения операций при использовании карточки предполагает наличие временного разрыва между датой совершения операции и отражения данной операции по Счету. Продолжительность периода между днем совершения операции и днем отражения операции по счету зависит от места осуществления операции (на территории Республики Беларусь или за границей), принадлежности технической инфраструктуры (Кредитодателю или другому банку), времени осуществления операции (ночное или дневное время, рабочие или выходные, праздничные дни).

В зависимости от страны пребывания и банка при проведении операции при использовании карточки может удерживаться дополнительное вознаграждение, о размерах которого целесообразно поинтересоваться у обслуживающего вас работника перед совершением операции либо заранее изучив информацию банка на его официальном сайте. Также такая информация может быть отображена на экране банкомата или устройства самообслуживания при совершении операции.

В случае если вы все же пострадали от мошенничества, необходимо немедленно заблокировать карточку и обратиться в Кредитодателю. По факту мошенничества необходимо подать заявление в правоохранительные органы.