**Материалы по теме « повышение финансовой грамотности населения» для потребителей банковских услуг**

**Банковская карта** - это финансовый инструмент (ключ), дающий возможность доступа и пользования денежными средствами, находящимися на личном банковском счете. Банковская карта предназначена для доступа к личному счету, открытому банком физическому или юридическому лицу. Банковская карта позволяет оплачивать товары и услуги, переводить денежные средства со одного своего счета на другой, а также получать наличные денежные средства в пределах остатка на личном счете или в пределах предоставленной банком кредитной линии или овердрафта.

**Держателем** карты является лицо, на имя которого выпущена карта, как правило, имя
и фамилия держателя указано на лицевой стороне карты - это персонализированная карта.
Карта может быть неперсонализированная. то есть на ней не указано имя держателя карты.
Обычно такие карты выпускаются банками под программы кредитования,

предусматривающие очень быстрое одобрение и выдачу кредита, иногда и в момент вашего первого обращения в банк. В этом случае держателем карты является лицо, которое заключило договор с банком, на имя которого открыт соответствующий счет в банке. Предъявить карту к оплате имеет право только держатель карты.

**Собственником карты** является банк её выпустивший, т.е. банк эмитент, и выдавший её в пользование держателю.

**Эмитент** - кредитная организация, осуществляющая эмиссию банковских карт.

**Эмиссия банковских карт** - деятельность, связанная с выпуском и(или) выдачей карт, а также с открытием счетов и расчетно-кассовым обслуживанием клиентов при совершении операций с использованием выданных им банковских карт.

**Авторизация** - разрешение, предоставляемое эмитентом для проведения операций с использованием платежных карт и порождающее обязательство по исполнению представленных документов, составленных с их использованием.

**Транзакция** - операция, совершенная с использованием банковской карты в торговой сети, банкоматах, пунктах выдачи наличных.

**Персональный идентификационный номер (ПИН-код)** - четырехзначный идентификационный номер клиента, присваиваемый каждой карте и используемый для идентификации держателя при совершении операций с использованием карты. Выдается клиенту вместе с картой в ПИН-конверте.

**Слип** - документ, формирующийся в торгово-сервисных предприятиях и пунктах выдачи наличных, удостоверяющий факт осуществления платежа/снятия наличных денежных средств по банковской карте.

Все карты, эмитируемые банком, имеют признаки принадлежности банку, логотип международной платежной системы, а также предусмотренные правилами платежной системы защитные признаки.

На каждую карту наносятся следующие данные:

идентификационный номер карты;

месяц и год окончания срока действия карты:

защитный символ - спецлитера (например, стилизованная буква "V" - по картам международной платежной системы Visa):

а также могут быть на нанесены имя (или инициалы) и фамилия держателя карты латинскими буквами.

Виды карт.

Расчетная (дебетовая) карта предназначена для совершения операций её держателем в пределах остатка денежных средств клиента, находящихся на его банковском счете с учетом установленных лимитов.

Продолжение развития дебетовых карт - это расчетные карты с разрешенным овердрафтом.

Овердрафт - кредит, предоставленный клиенту банка в случае недостаточности или отсутствия денежных средств на счете при осуществлении расчетных операций по банковской карте. Обычно овердрафт предоставляется на непродолжительный срок (обычно 30-50 дней) клиентам, имеющим регулярные денежные поступления на этот счет, т.е. в конкретный момент предоставления овердрафта средств клиента недостаточно для оплаты текущих расходов

В классическом виде карты с овердрафтом выпускаются на базе зарплатных карт, а размер овердрафта составляет от 50 до 200% среднемесячных поступлений на счет.

**Предоплаченная карта** предназначена для совершения её держателем операций, расчеты по которым осуществляются кредитной организацией-эмитентом от своего имени, и удостоверяет право требования держателя предоплаченной карты к кредитной организации-эмитенту по оплате товаров (работ, услуг) или выдаче наличных денежных средств.

**Кредитные карты** позволяют их держателям распоряжаться денежными средствами, предоставленными банком клиенту согласно условиям кредитного договора.

Отличие кредитных карт от карт с разрешенным овердрафтом в невозможности по кредитной карте иметь положительный остаток.

Это становится важно в случае погашения задолженности по кредиту. То есть, если клиент внес на кредитную карту сумму больше, чем сумма его задолженности, то излишняя часть учитывается на отдельном счёте и не может быть использована на совершение операций за счет средств клиента. Она пойдет только на будущее погашение кредита после его возникновения. Причем кредит гасится в определённую дату, оговоренную договором, а не сразу после возникновения.

Отличие кредитных карт от потребительских кредитов, которые могут перечисляться на расчетную карту, состоит в том, что:

1. В отчете о расходовании кредита. В случае кредитной карты не надо отчитываться перед банком о целевом использовании взятого кредита, при потребительском - может потребоваться предоставление отчета банку.
2. В характере кредита. По кредитной карте существует возможность постоянного возобновления кредитной линии после погашения задолженности. В случае зачисления потребительского кредита на расчетную карту предоставление кредитных средств является лишь разовым зачислением, повторно воспользоваться кредитом уже нельзя.
3. В начислении процентов по кредиту. По кредитной карте проценты за использование кредита начисляются лишь, когда клиент начинает использовать карту и кредитные средства на ней, в случае потребительского кредита, зачисляемого на карту банк начинает начислять проценты с даты заключения кредитного договора и перечисления средств на счет карты, то есть как только они стали доступны клиенту.

**Классификация по сервисам:**

**Массовые карты** - электронные (Electron. Maestro). Могут использоваться только в электронных устройствах - банкоматах, электронных POS-терминалах. Как правило ими невозможно оплачивать услуги в Интернет, использовать при бронировании гостиниц, при оплате через импринтер. Электронные карты часто используются для выдачи зарплаты, получения процентов по вкладам, погашения кредитов. По электронным картам банки обычно устанавливают меньшие лимиты дневного снятия наличных, и при малом наборе услуг стоимость годового обслуживания минимальна или бесплатна. Данные карты оптимальны для держателей пользующихся в основном для снятия наличных средств и совершения редких покупок картой.

Классические **карты** (Classic. Standard) - позволяют совершать любые банковские операции, предусмотренные для карт. Могут иметь кредитный лимит, использоваться по всему миру. Карты предоставляются физическим лицам со стабильным ежемесячным доходом, имеющим положительную репутацию и кредитную историю.

**Премиальные карты** - помимо стандартного набора сервисов держателю доступны дополнительные услуги: экстренная помощь при утере или краже карты, экстренная замена карты, экстренная выдача наличных средств (пакет услуг в зависимости от банка-эмитента и платежной системы). **Например, Gold/Platinum:** карты выпускаются наиболее привилегированным клиентам, имеющим высокий ежемесячный доход, положительную кредитную историю, минимальный риск невозврата платежей и т.п.

Банком России в рамках работы по информированию о рисках, связанных с использованием банковских карт, и повышению финансовой грамотности населения подготовлена Памятка «О мерах безопасного использования банковских карт» (Письмо Банка России от 2.10.2009 № 120-Т).

Соблюдение рекомендаций, содержащихся в Памятке, позволит обеспечить максимальную сохранность банковской карты, ее реквизитов. ПИН и других данных, а также снизит возможные риски при совершении операций с использованием банковской карты в банкомате, при безналичной оплате товаров и услуг, в том числе через сеть Интернет.

**Общие рекомендации**

1. Никогда не сообщайте ПИН третьим лицам, в том числе родственникам, знакомым, сотрудникам кредитной организации, кассирам и лицам, помогающем Вам в использовании банковской карты.

•2. ПИН необходимо запомнить или в случае, если это является затруднительным, хранить его отдельно от банковской карты в неявном виде и в недоступном для третьих лиц. в том числе родственников, месте нахождения.

1. Никогда ни при каких обстоятельствах не передавайте банковскую карту для использования третьим лицам, в том числе родственникам. Если на банковской карте нанесены фамилия и имя физического лица, то только это физическое лицо имеет право использовать банковскую карту.
2. При получении банковской карты распишитесь на ее оборотной стороне в месте, предназначенном для подписи держателя банковской карты, если это предусмотрено. Это снизит риск использования банковской карты без Вашего согласия в случае ее утраты.
3. Будьте внимательны к условиям хранения и использования банковской карты. Не подвергайте банковскую карту механическим, температурным и электромагнитным воздействиям, а также избегайте попадания на нее влаги. Банковскую карту нельзя хранить рядом с мобильным телефоном, бытовой и офисной техникой.
4. Телефон кредитной организации - эмитента банковской карты (кредитной организации, выдавшей банковскую карту) указан на оборотной стороне банковской карты.

Необходимо всегда иметь при себе контактные телефоны кредитной организации - эмитента банковской карты (её call-центра) и номер банковской карты на других носителях информации: занесите их в записную книжку, мобильный телефон и/или другие носители информации, но не рядом с записью о ПИН.

1. С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета целесообразно установить суточный лимит на сумму операций по банковской карте и одновременно подключить электронную услугу оповещения о проведенных операциях (например, оповещение посредством SMS-сообщений или иным способом). При смене личного номера мобильного телефона обязательно уведомите банк, чтобы информация по вашей карте не стала доступным посторонним лицам, в случае если у вас подключена услуга «мобильный банк», и сделайте это немедленно.
2. В целях информационного взаимодействия с кредитной организацией - эмитентом банковской карты (кредитной организации, выдавшей банковскую карту) рекомендуется использовать только реквизиты средств связи (мобильных и стационарных телефонов, факсов, интерактивных web-сайтов/порталов, обычной и электронной почты и пр.). которые указаны в документах, полученных непосредственно в кредитной организации - эмитенте банковской карты.
3. При получении просьбы, в том числе со стороны сотрудника кредитной организации (а также поступившей посредством e-mail и sms-соообшений) сообщить персональные данные или информацию о банковской карте (в том числе ПИН) не сообщайте их. Перезвоните в кредитную организацию - эмитент банковской карты (кредитную организацию, выдавшую банковскую карту) и сообщите о данном факте.
4. Не рекомендуется отвечать на электронные письма, в которых от имени кредитной организации (в том числе кредитной организации - эмитента банковской карты (кредитной организации, выдавшей банковскую карту) предлагается предоставить персональные данные. Не следуйте по "ссылкам", указанным в этих письмах (включая ссылки на сайт кредитной организации), т.к. они могут вести на сайты-двойники.
5. Помните, что в случае раскрытия ПИН, персональных данных, утраты банковской карты существует риск совершения неправомерных действий с денежными средствами на Вашем банковском счете со стороны третьих лиц.

В случае если имеются предположения о раскрытии ПИН, персональных данных, позволяющих совершить неправомерные действия с Вашим банковским счетом, а также если банковская карта была утрачена, необходимо немедленно обратиться в кредитную организацию - эмитент банковской карты (кредитную организацию, выдавшую банковскую карту) и следовать указаниям сотрудника данной кредитной организации. До момента

обращения в кредитную организацию - эмитент банковской карты Вы несете риск, связанный с несанкционированным списанием денежных средств с Вашего банковского счета. Как правило, согласно условиям договора с кредитной организацией - эмитентом банковской карты денежные средства, списанные с Вашего банковского счета в результате несанкционированного использования Вашей банковской карты до момента уведомления об этом кредитной организации - эмитента банковской карты, не возмещаются.

**Рекомендации при совершении операций** с **банковской картой в банкомате**

1. Осуществляйте операции с использованием банкоматов, установленных в безопасных местах (например, в государственных учреждениях, подразделениях банков, крупных торговых комплексах, гостиницах, аэропортах и т.п.).
2. Не используйте устройства, которые требуют ввода ПИН для доступа в помещение, где расположен банкомат.
3. В случае если поблизости от банкомата находятся посторонние лица, следует выбрать более подходящее время для использования банкомата или воспользоваться другим банкоматом.
4. Перед использованием банкомата осмотрите его на наличие дополнительных устройств, не соответствующих его конструкции и расположенных в месте набора ПИН и в месте (прорезь), предназначенном для приема карт (например, наличие неровно установленной клавиатуры набора ПИН). В указанном случае воздержитесь от использования такого банкомата.
5. В случае если клавиатура или место для приема карт банкомата оборудованы дополнительными устройствами, не соответствующими его конструкции, воздержитесь от использования банковской карты в данном банкомате и сообщите о своих подозрениях сотрудникам кредитной организации по телефону, указанному на банкомате.
6. Не применяйте физическую силу, чтобы вставить банковскую карту в банкомат. Если банковская карта не вставляется, воздержитесь от использования такого банкомата.
7. Набирайте ПИН таким образом, чтобы люди, находящиеся в непосредственной близости, не смогли его увидеть. При наборе ПИН прикрывайте клавиатуру рукой.
8. В случае если банкомат работает некорректно (например, долгое время находится в режиме ожидания, самопроизвольно перезагружается), следует отказаться от использования такого банкомата, отменить текущую операцию, нажав на клавиатуре кнопку "Отмена", и дождаться возврата банковской карты.
9. После получения наличных денежных средств в банкомате следует пересчитать банкноты полистно, убедиться в том, что банковская карта была возвращена банкоматом.

дождаться выдачи квитанции при ее запросе, затем положить их в сумку (кошелек, карман) и только после этого отходить от банкомата.

1. Следует сохранять распечатанные банкоматом квитанции для последующей сверки указанных в них сумм с выпиской по банковскому счету.
2. Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций с банковской картой в банкоматах.
3. Если при проведении операций в банкомате с использованием банковской карты банкомат не возвращает карту, следует позвонить в кредитную организацию по телефону, указанному на банкомате, и объяснить обстоятельства произошедшего, а также следует обратиться в кредитную организацию - эмитент банковской карты (кредитную организацию, выдавшую банковскую карту), которая не была возвращена банкоматом, и далее следовать инструкциям сотрудника кредитной организации.

**Рекомендации при использовании банковской карты для безналичной оплаты**

**товаров и услуг**

1. Не используйте банковские карты в организациях торговли и услуг, не вызывающих доверия.
2. Требуйте проведения операций с банковской картой только в Вашем присутствии. Это необходимо в целях снижения риска неправомерного получения Ваших персональных данных, указанных на банковской карте.
3. При использовании банковской карты для оплаты товаров и услуг кассир может потребовать от владельца банковской карты предоставить паспорт, подписать чек или ввести ПИН. Перед набором ПИН следует убедиться в том, что люди, находящиеся в непосредственной близости, не смогут его увидеть. Перед тем как подписать чек, в обязательном порядке проверьте сумму, указанную на чеке.
4. В случае если при попытке оплаты банковской каргой имела место "неуспешная" операция, следует сохранить один экземпляр выданного терминалом чека для последующей проверки на отсутствие указанной операции в выписке по банковскому счету.

**Рекомендации при совершении операций с банковской картой через сеть Интернет**

1. Не используйте ПИН при заказе товаров и услуг через сеть Интернет, а также по телефону/факсу.
2. Не сообщайте персональные данные или информацию о банковской(ом) карте (счете) через сеть Интернет, например ПИН, пароли доступа к ресурсам банка, срок действия банковской карты, кредитные лимиты, историю операций, персональные данные.

3. С целью предотвращения неправомерных действий по снятию всей суммы
денежных средств с банковского счета рекомендуется для оплаты покупок в сети Интернет
использовать отдельную банковскую карту (так называемую виртуальную карту) с
предельным лимитом, предназначенную только для указанной цели и не позволяющую
проводить с ее использованием операции в организациях торговли и услуг.

Виртуальная карта (например. Visa Virtuon или MasterCard Virtual) предназначена для клиентов банка, приобретающих товары и услуги в сети Интернет, и позволяет, в отличие от классических пластиковых карт, сделать данные платежи более безопасными. Клиенту открывается в банке специальный карточный счет, по которому устанавливается ежемесячное ограничение суммы расходов до определенной суммы.

Виртуальную карту нельзя использовать в обычной торгово-сервисной сети или в банкоматах.

Внести денежные средства на виртуальную карту можно в любом отделении (филиале) банка-эмитента или банковским переводом. Получить остаток денежных средств по карте возможно только в случае её закрытия при обращении в отделение (филиал) банка-эмитента. В целях безопасности срок действия виртуальных карт ограничен - 6 месяцев. Виртуальная карта также может быть открыта как дополнительная к обычной банковской карте.

1. Следует пользоваться интернет-сайтами только известных и проверенных организаций торговли и услуг.
2. Обязательно убедитесь в правильности адресов интернет-сайтов, к которым подключаетесь и на которых собираетесь совершить покупки, т.к. похожие адреса могут использоваться для осуществления неправомерных действий.
3. Рекомендуется совершать покупки только со своего компьютера в целях сохранения конфиденциальности персональных данных и(или') информации о банковской(ом) карте (счете).

В случае если покупка совершается с использованием чужого компьютера, не рекомендуется сохранять на нем персональные данные и другую информацию, а после завершения всех операций нужно убедиться, что персональные данные и другая информация не сохранились (вновь загрузив в браузере web-страницу продавца, на которой совершались покупки).

7. Установите на свой компьютер антивирусное программное обеспечение и
регулярно производите его обновление и обновление других используемых Вами
программных продуктов (операционной системы и прикладных программ), это может
защитить Вас от проникновения вредоносного программного обеспечения.

**Оформление заявлений в кредитную организацию при несогласии с совершенными операциями**

При написании заявления необходимо подробно описать всю хронологию событий -например, для описания операции снятия наличных в банкомате: что делали, какую сумму запрашивали, какую получили, что происходило с банкоматом, какие меры предпринимали, куда позвонили и что Вам ответили. Не лишним будет сохранить для себя все копии написанных заявлений с пометками об их принятии, при этом на полях, можно записать имена и телефоны специалистов, с которыми пришлось общаться. Обращаться необходимо в банк, выпустивший Вашу банковскую карту - по телефону, указанному на оборотной стороне и лично в офис банка, а также по номеру телефона, указанному на банкомате, в случае, если денежные средства снимаются в банкомате банка-эквайрера.

**Мошеннические операции с картами**

История злоупотреблений с платежными картами началась с момента их появления. Тогда же появились и первые простейшие подделки.

В конце 70-х гг. появилась очень распространенная сегодня схема мошенничества, получившая название «белый пластик». Номера настоящих карточек эмбосировались (процесс теснения. формирования рельефных, выступающих над поверхностью карты символов) на заготовках пластиковых карт, не имевших «опознавательных знаков» банка и платежной системы (отсюда и название - «белый пластик»). Чтобы воспользоваться «белым пластиком», преступникам приходилось вступать в сговор с кассирами торговых предприятий. Кассиры делили с мошенниками доходы от операции после оплаты с фальшивого счета банком.

На сегодняшний день наиболее распространенными являются следующие способы мошенничества с использованием карт.

1. **Хищения, совершаемые при помощи подлинных платежных карт.**

Их особенностью является то. что при совершении преступлений злоумышленникам известен ПИН владельца карты. Для совершения используются следующие технологии:

1.1. Установка ливанской петли на картоприемник банкомата.

* преступниками изготавливается из фотопленки или другого тонкого, но прочного, гибкого материала специальный кармашек в цвет принимающего карту окошка в банкомате, длиной около 20 см;
* преступник устанавливает данное устройство в щель картридера. закрепляя концы устройства снаружи таким образом, чтобы держатель карты без подозрений мог вставить банковскую карту в щель картридера;
* в непосредственной близости от банкомата преступник поджидает потенциального потерпевшего;
* держатель карты, завершив все операции, пытается получить карту обратно, однако устройство, установленное преступником в банкомат, не позволяет сделать этого. В этот момент преступник подходит к держателю карты и под предлогом оказания помощи узнает ПИН.

Как правило, такие преступления совершаются в ночное время либо в местах, где мобильная связь недоступна, чтобы клиент не смог дозвониться в сервисную службу, и после того, как владелец карты уходит, преступник извлекает устройство вместе с его банковской картой и с помощью этого же банкомата присваивает все денежные средства, находящиеся на счете клиента банка.

1. Подглядывание мошенником значения ПИН при его наборе на клавиатуре банкомата держателем карты. Узнав ПИН. злоумышленники пытаются завладеть картой, как правило, с помощью карманной кражи либо грабежа.
2. Снятие денежных средств при помощи украденной либо утерянной карты. Подобное возможно, когда ПИН либо нанесен владельцем на самой карте, либо написан на бумажке и хранится вместе с картой в бумажнике или сумочке, либо внесен в записную книжку телефона, и эти предметы одновременно оказались у преступников.

1.4. Несанкционированное снятие денежных средств при помощи карты,
принадлежащей владельцу, доверившему ее третьему лицу для проведения операций.

2. Хищения, совершаемые при помощи поддельных платежных карт.

Для совершения указанных видов преступлений злоумышленникам не требуется банковская карта владельца. Достаточно знать данные с магнитной полосы и ПИН карты. В настоящее время для получения данных о платежной карте преступниками применяются современные технические средства.

При этом могут использоваться:

1. Поддельные банкоматы, в которых установлены устройства, считывающие реквизиты банковской карты и записывающие ПИН код;
2. Настоящие банкоматы - с целью получения информации о платежной карте. Преступниками устанавливаются на банкомате следующие технические устройства:

а) предназначенные для снятия информации с магнитной полосы платежной карты:

- так называемый скиммер, - техническое устройство, имитирующее приемное

отверстие банкомата и устанавливаемое поверх него. При установке карты в имитирующее

приемное отверстие банкомата производится считывание информации ("дамп"),

содержащейся на магнитной полосе карты. Скиммеры бывают разных форм, расцветок и

размеров - от пластинок длиной 1,5 см и шириной 5 мм до накладных пластин размером 40 х 40 мм;

- приемное устройство, на которое посредством радиосвязи преступник получает
"дамп" платежной карты;

б) устройства для определения ПИН:

* накладная клавиатура - устанавливается поверх настоящей клавиатуры банкомата. При нажатии на клавиши фальшь-клавиатуры импульсы передаются на настоящие клавиши, а также на экран банкомата и по радиосвязи - на передающее устройство, вследствие чего преступники узнают ПИН;
* мини-видеокамера, с помощью которой преступники получают видеокартинку **с** информацией о вводимом ПИН. Мини-видеокамера маскируется на корпусе банкомата под различные предметы, не вызывающие подозрений, например под коробочку для размещения рекламных буклетов.

После получения информации с магнитной полосы и значения ПИН преступники изготавливают поддельную платежную карту, реквизиты которой полностью повторяют реквизиты реальной платежной карты, выпущенной эмитентом, и снимают деньги в настоящих банкоматов.

2.3. Новые способы завладения денежными средствами из банкоматов, такие как применение вредоносного программного обеспечения, которое устанавливается на жесткий диск компьютера, осуществляющего управление банкоматом.

**3. Хищения, совершаемые через предприятия торговли, принимающие
банковские карты в качестве средства платежа.**

Для осуществления указанных преступлений используются следующие приемы:

1. При помощи POS-терминала работником предприятия торговли делается более одной проводки платежной карты для подготовки других платежных документов или увеличения суммы в платежном документе, подписанном клиентом.
2. Метод повторения электронных слипов. Он отличается от предыдущего метода тем. что осуществляется с использованием электронного терминала. Этот метод особенно распространен при ручном вводе реквизитов карты.
3. Перехват счета магазина. В этом случае мошенники от имени торгового предприятия извещают банк об изменении расчетного счета для перечисления средств по совершенным операциям.

**4. Хищения, совершаемые со счетов держателей платежных карт без
фактического использования банковской карты.**

Такого рода хищения возможны при проведении CNP-транзакций (транзакции Card Not Present) - операций с "карточными" счетами клиентов банков посредством применения реквизитов платежных карт, но без их фактического использования. Мошенничество основывается на использовании платежных реквизитов банковской карты, включая дополнительный код безопасности карты, не ее законным держателем **при** оплате в интернет-магазинах и торговых точках, оформляющих заказы дистанционно.

**5. Хищения с использованием систем «мобильный банк».**

При совершении указанных видов преступлений сам телефон или номер мобильного телефона, привязанный к счету карты держателя, становится доступным для мошенников. В этом случае, путем направления смс-сообщений в адрес банка, мошенник может распоряжаться денежными средствами, находящимися на карточном счете держателя.