

**Приложение № 4.1 к Договору о комплексном  
банковском обслуживании клиентов-физических  
лиц в Акционерном обществе «Черноморский  
банк развития и реконструкции» (новая редакция)**

**ПРАВИЛА пользования картой**

Требования по соблюдению мер безопасности, содержащихся в настоящих Правилах пользования картой (далее в настоящем Приложении – Правила), являются обязательными и направлены на предотвращение возникновения финансовых потерь у Держателя банковской расчетной карты (далее – карта и Клиент, соответственно) в результате совершения противоправных действий с использованием карты. В случае нарушений Клиентом Правил, например, при разглашении ПИН-кода, реквизитов карты, персональных данных Клиента, а также в случае утраты карты, карта становится источником повышенного риска несанкционированного списания денежных средств с карточного счета Клиента.

В результате нарушения Правил, неправомерно полученные сведения о реквизитах карты могут быть использованы мошенниками для совершения несанкционированных Клиентом операций, для изготовления поддельных карт, частично или полностью имитирующих подлинные, следствием чего являются финансовые потери Клиента.

**1. Общие правила безопасности**

- 1.1. При получении новой карты Клиент обязан проставить свою подпись на оборотной стороне карты на полосе для подписи.
- 1.2. Клиент обязан хранить в секрете ПИН-код (персональный идентификационный номер) и реквизиты карты (номер карты, срок действия, код защиты CVC2 – трехзначный код, указанный на оборотной стороне карты). Клиент никогда не должен сообщать ПИН-код третьим лицам, в том числе родственникам, знакомым, сотрудникам банков, кассирам и лицам, помогающим ему в использовании карты. Запрещается записывать ПИН-код на карте и хранить его рядом с картой. Запрещается записывать ПИН-код в память мобильного телефона без его шифрования или без установления соответствующей блокировки телефона.
  - 1.2.1. Несоблюдение данного правила приводит к тому, что по карте, похищенной вместе с телефоном, содержащим сведения о ПИН-коде, мошенники получают полный доступ к денежным средствам Клиента.
- 1.3. Передача карты для использования третьим лицам, в том числе родственникам является нарушением Правил. Если необходимо, для доверенных лиц Клиента может быть выпущена дополнительная карта.

Договор о комплексном банковском обслуживании физических лиц в  
Акционерном обществе «Черноморский банк развития и реконструкции»  
(новая редакция)

- Использовать карту имеет право только лицо, имя которого указано на карте.
- 1.4. Запрещается предоставлять посторонним лицам сведения о своих персональных данных, реквизитах карты и (или) ПИН-коде в ответах на электронные письма, SMS-сообщения или звонки, в которых от имени Банка предлагается предоставить такие данные. В случае сомнений, что звонок или сообщение исходят из Банка, следует самостоятельно перезвонить по телефону, указанному на обороте карты в службу поддержки держателей карт Банка.
- 1.5. В целях информационного взаимодействия с Банком следует использовать только реквизиты средств связи (номера телефонов, адреса обычной и электронной почты и пр.), которые указаны в документах, полученных непосредственно в Банке.
- 1.6. Клиент обязан проверять выписку по карточному счету, в которой указываются операции за отчетный период, не реже одного раза в месяц. Банк предоставляет возможность и настоятельно рекомендует подключить услугу оповещения о проведенных операциях посредством SMS-сообщений. В случае обнаружения подозрительных или неизвестных операций Клиент обязан немедленно сообщить об этом в Банк.
- 1.7. В целях предотвращения возникновения финансовых потерь у Клиента, Банк имеет право устанавливать и изменять лимиты безопасности на проведение операций с использованием карт, в том числе на получение наличных денежных средств по карте в сторонних банках.
- 1.8. В случае утраты (кражи) карты и (или) ПИН-кода, а также в случае риска возникновения несанкционированного использования карты, ее реквизитов и (или) ПИН-кода, Клиент обязан незамедлительно уведомить об этом Банк одним из следующих способов:
- 1.8.1. по номерам телефонов, указанным на обратной стороне карты;
- 1.8.2. обратившись в любое Подразделение Банка.
- 1.9. Необходимо всегда иметь при себе контактные телефоны Банка. До момента обращения в Банк Клиент несет риск, связанный с несанкционированным списанием денежных средств с карточного счета.
- 1.9.1. Контактные телефоны Клиентской поддержки по операциям с картами:
- +7 (978) 099 03 80 (нерабочие часы Банка) – Блокировка/разблокировка карт.
- +7 (978) 835 27 27 (понедельник – пятница с 9:00 до 18:00)
- 1.9.2. Многоканальный телефонный номер Банка:
- 1.8.1.1.1. +7 (978) 099 03 80 – многоканальный
- 1.8.1.1.2. +7 (3652) 605-805 – многоканальный

Договор о комплексном банковском обслуживании физических лиц в  
Акционерном обществе «Черноморский банк развития и реконструкции»  
(новая редакция)

- 1.10. В случае совершения противоправных действий против Клиента с целью завладения картой, ПИН-кодом, реквизитами карты, Клиенту следует незамедлительно обратиться в ближайший отдел полиции.
- 1.11. Клиент обязан внимательно относиться к условиям хранения и использования карты, предотвращать механическое, температурное и электромагнитное воздействие на карту, избегать попадания на нее влаги. Запрещается хранить карту рядом с мобильным телефоном, бытовой и офисной техникой.
- 1.12. Банк имеет право приостановить или полностью прекратить действие карты в случае возникновения подозрений в компрометации карты, а также восстановить действие карты при устранении причин приостановления ее действия.
- 1.13. Банк уведомляет Клиента в день приостановления (прекращения) действия Карты (с указанием причины приостановления/прекращения действия Карты) одним из следующих способов:
- 1.13.1. путем уведомления по номеру телефона, указанному в Заявлении о предоставлении и использовании банковской расчетной карты;
  - 1.13.2. путем направления SMS-сообщения по номеру телефона, указанному в Заявлении о предоставлении и использовании банковской расчетной карты;
  - 1.13.3. путем направления уведомления по адресу электронной почты, указанному в Заявлении о предоставлении и использовании банковской расчетной карты;
  - 1.13.4. путем направления электронного уведомления по Системе ДБО ФЛ;
  - 1.13.5. путем направления письменного уведомления заказным письмом по адресу, указанному в Заявлении о предоставлении и использовании банковской расчетной карты.
- 1.14. В целях предотвращения возникновения финансовых потерь у Клиента при наборе неверного ПИН-кода три раза подряд, действие карты блокируется. Разблокировать карту держатель карты может одним из следующих способов:
- 1.14.1. по номерам телефонов, указанным на оборотной стороне карты и в п.1.8 Правил;
  - 1.14.2. обратившись в Подразделение Банка.

**2. Правила безопасности при совершении операций с картой в банкомате**

- 2.8. До совершения операции следует обратить внимание на внешний вид банкомата. Запрещается совершать операции при обнаружении любых внешних признаков неисправности банкомата или обнаружении рядом с ним или на нем посторонних устройств, накладных панелей, инородных предметов

Договор о комплексном банковском обслуживании физических лиц в  
Акционерном обществе «Черноморский банк развития и реконструкции»  
(новая редакция)

- в (на) картоприемнике, клавиатуре банкомата, отверстии для выдачи наличных. При обнаружении посторонних устройств и предметов следует сообщить об этом в Банк, и воспользоваться другим банкоматом.
- 2.9. Если Карта не вставляется в банкомат, запрещается применять физическую силу чтобы вставить карту, следует воздержаться от использования такого банкомата.
- 2.10. Не следует использовать устройства, которые требуют ввода ПИН-кода для доступа в помещение, где расположен банкомат. Следует использовать банкоматы, установленные в безопасных местах (например, в государственных учреждениях, подразделениях банков, крупных торговых комплексах, гостиницах, аэропортах и т. п.). Следует избегать использования банкоматов в плохо освещенных и безлюдных местах.
- 2.11. 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 карты.
- 2.12. Не допускайте присутствия сторонних лиц при проведении операции. При наличии установленных на банкомате специальных зеркал наблюдения воспользуйтесь ими для снижения риска несанкционированного наблюдения третьими лицами за проведением Вами операции. Следует убедиться в том, что люди, стоящие рядом с Вами, не имеют возможности увидеть ПИН-код или сумму снимаемых наличных. При наборе ПИН-кода на банкоматах, не оборудованных закрывающей клавиатуру защитной шторкой, прикрывайте клавиатуру рукой.
- 2.13. При совершении операций с картой запрещается руководствоваться советами третьих лиц. В случае возникновения каких-либо проблем при совершении операции (например, банкомат не возвращает карту) следует незамедлительно обратиться в Банк по номерам телефонов Банка, объяснить обстоятельства произошедшего и следовать инструкциям сотрудника Банка.
- 2.14. Если банкомат стороннего банка не возвращает карту, то Клиенту следует:
- 2.14.1.0. по телефону, указанному на банкомате, обратиться в банк – владелец банкомата и выяснить сроки и порядок возврата карты;
- 2.14.1.1. по телефону Банка заблокировать карту, т. к. карта, находящаяся не на руках ее держателя, не должна быть активной.
- 2.15. При проведении операции не следует отходить от банкомата. Возвращённую банкоматом карту следует немедленно убрать в сумку (кошелек, карман), полученные наличные денежные средства пересчитать поштучно, убрать их, дождаться выдачи квитанции при ее запросе, и только

после этого отходить от банкомата.

- 2.16. Следует сохранять распечатанные банкоматом квитанции для последующей сверки указанных в них сумм с выпиской по карточному счету.
- 2.17. Банкоматы выдают денежные купюры определенного номинала. Необходимая сумма денежных средств выбирается из предлагаемого набора меню Банкомата либо вводится Держателем. Вводимая сумма должна быть кратной номиналам купюр и не может превышать максимальную сумму, указанную на Банкомате или ограниченную Платежным лимитом. В противном случае будет выдано сообщение об ошибочной сумме.
- 2.18. Держатели имеют возможность оплачивать/подключать через Банкоматы ряд услуг из предлагаемого набора в меню Банкомата, а также получать информацию об остатке денежных средств на Карте, осуществлять переводы денежных средств по Карте. Набор услуг и возможность предоставления информации о состоянии Карты определяет Банк-эквайер.

### **3. Правила безопасности при использовании карты для безналичной оплаты товаров и услуг**

- 3.1. Перед оплатой товаров (услуг) Клиент сообщает служащему (кассиру) Торговой точки о том, что будет производить оплату по Карте.
- 3.2. При использовании карты для оплаты товаров и услуг кассир может потребовать от владельца карты подписать чек и (или) ввести ПИН-код, предъявить документ, удостоверяющий личность. При наборе ПИН-кода следует прикрывать клавиатуру рукой. Перед подписанием чека следует обязательно проверить сумму, указанную на чеке, а при получении SMS-сообщения, информирующего о совершенной операции, проверить сумму фактического списания с Карточного счета.
- 3.3. В случае выпуска Держателю банковской карты со встроенным электронным микропроцессором при совершении операции может осуществляться идентификация Держателя в соответствии с информацией о нем, содержащейся на чипе.
- 3.4. В случае выпуска Держателю Карты с бесконтактным чипом, который позволяет осуществлять операции по Карте путем приложения Карты к считывающему устройству на основе технологии бесконтактной оплаты, предлагаемой Платежной системой при совершении операции, сумма которой не превышает 3 000 (три тысячи) рублей, ПИН-код/собственноручная подпись Держателя может не запрашиваться. При совершении любой операции по Карте, оснащенной бесконтактным чипом, осуществляется обязательная электронная Авторизация. Возможность

опротестования указанных операций не предусмотрена.

3.5. После проведения операции Терминал распечатывает два экземпляра чека, один из которых предназначен для Клиента, а второй – для служащего (кассира) Торговой точки. Необходимо проверить правильность указанных на чеках данных и проставить свою подпись (если иное не оговорено настоящими Правилами).

3.5.1. В случае если чек распечатан не был или был распечатан не полностью, служащий (кассир) Торговой точки производит печать дубликата чека (на чеке указывается, что это копия), при этом недопустимо повторное проведение операции с использованием Карты через Терминал, так как это приведет к уменьшению суммы доступного Платежного лимита, повторному оформлению и списанию с Карточного счета суммы платежа.

3.6. При списании с Карточного счета суммы большей, чем стоимость покупки (услуги), либо при отказе Клиента от приобретения товара (услуги) после совершения платежа с использованием Карты Клиент в случаях, предусмотренных действующим законодательством, вправе требовать (непосредственно после совершения операции) отмены операции. Отмену операции производит служащий (кассир) Торговой Точки.

3.6.1. В этих случаях Держателю следует получить от Торговой точки и сохранить Документ, содержащий реквизиты отмененной операции (номер Карты, дату и время совершения отмененной операции, Код авторизации, сумму операции и сумму возврата). Документ подлежит хранению в течение одного месяца со дня совершения операции.

3.7. Не используйте Карту в организациях торговли и услуг, если торговая точка и (или) ее персонал не вызывают у Вас доверия.

3.8. В случае если при попытке оплаты картой имела место «неуспешная» операция, следует сохранять выданный терминалом чек, свидетельствующий о неуспешном завершении операции, для последующей проверки отсутствия указанной операции в выписке по Карточному счету.

#### **4. Правила безопасности при совершении операций по карточному счету через сеть Интернет**

4.1. При совершении операций по Карточному счету через сеть Интернет существует риск получения мошенниками персональных данных Клиента (в том числе паролей, реквизитов Карты и Карточного счета), в том числе:

4.1.1. путем рассылки электронных писем от имени банков, популярных

Договор о комплексном банковском обслуживании физических лиц в  
Акционерном обществе «Черноморский банк развития и реконструкции»  
(новая редакция)

- брендов, различных сервисов (Rambler, Mail.ru) или внутри социальных сетей с требованием ввести либо подтвердить свои персональные данные под различными предложениями;
- 4.1.2.с помощью специальных вредоносных программ (вирусов), которые позволяют получить доступ ко всей информации, вводимой в компьютер.
- 4.2. С целью снижения таких рисков запрещается:
- 4.2.1.следовать по ссылкам, указанным в подобных электронных письмах (включая ссылки на Официальный сайт Банка), т. к. они могут вести на сайты-двойники;
- 4.2.2.сообщать ПИН-код через сеть Интернет;
- 4.2.3.сообщать свои персональные данные или информацию о Карте (Карточном счете) через сеть Интернет, например, пароли доступа к ресурсам Банка, кредитные лимиты, историю операций, персональные данные;
- 4.2.4.совершать покупки с чужого компьютера.
- 4.3. Клиент обязан установить на свой компьютер антивирусное программное обеспечение и регулярно производить его обновление и обновление других используемых программных продуктов (операционной системы и прикладных программ).
- 4.4. Клиент обязан настроить операционную систему на своем компьютере так, чтобы обеспечивались основные правила безопасности работы в сети.
- 4.5. С целью минимизации рисков, связанных с проведением неправомерных операций по Карточному счету, для оплаты покупок в сети Интернет предоставляется возможность и настоятельно рекомендуется:
- 4.5.1.либо использовать Карту с отдельным Карточным счетом, открытую только для осуществления покупок в сети Интернет и не размещать на таком Карточном счете денежные средства в сумме, значительно превышающей сумму предполагаемой операции;
- 4.6. При осуществлении покупок Клиент обязан пользоваться Интернет сайтами только известных и проверенных организаций торговли и услуг.
- 4.7. Клиент обязан убедиться в правильности адреса Интернет сайта, к которому подключается и на котором собирается совершить покупки, т.к. похожие адреса могут использоваться для осуществления неправомерных действий.
- 4.8. Перед совершением покупки Клиент обязан узнать больше информации об Интернет-магазине:
- 4.8.1.прочитать опубликованные на сайте правила работы с информацией личного характера. Обратить внимание на меры обеспечения Интернет-

магазином информационной безопасности;

- 4.8.2. убедиться в том, что Интернет-магазин использует подтвержденный сертификат для обеспечения информационной безопасности. Желательно подтверждение сертификата подлинности одним из всемирных доверенных сертификационных агентств, например, <http://www.verisign.com/> или <http://www.globalsign.com/>;
- 4.8.3. убедиться в наличии у Интернет-магазина фактического адреса и зарегистрированного юридического лица, эти данные должны быть указаны на сайте;
- 4.8.4. ознакомиться с условиями поставки товара и правилами его возврата, правилами предоставления услуги, в том числе о дополнительных сборах;
- 4.8.5. проверить, есть ли на сайте Интернет-магазина форум, где посетители оставляют отзывы. Ознакомиться с отзывами о магазине на иных сайтах сети Интернет.
- 4.9. Для подтверждения операций оплаты товаров, работ и услуг в сети Интернет с применением Технологии 3-D Secure Держатель переадресовывается на специальный сайт, где Держателю необходимо ввести пароль, идентифицирующий личность Держателя. Одноразовый пароль передается Банком Держателю посредством SMS-сообщения. SMS-сообщение направляется Держателю на его Доверенный номер телефона<sup>1</sup>. Держатель несет ответственность за сохранение конфиденциальности одноразового пароля для подтверждения операции.
- 4.10. Клиент обязан сохранять конфиденциальность своего пароля и периодически менять его. Запрещается сохранять в системе пароли и сообщать свои пароли, используемые для входа на сайт Интернет-магазина, третьим лицам. Банк рекомендует не использовать просто вычисляемые пароли (например, дата рождения, номера телефона), а также использовать одинаковый пароль для Интернет-магазинов, своей почты и других систем.

---

<sup>1</sup> Предоставляемый Клиентом на условиях, указанных в приложении 4 к Комплексному договору.