Приложение № 2

к Правилам универсального банковского обслуживания
физических лиц в АО «Датабанк»
(на публичных условиях) (УДБО)»

ПРАВИЛА БЕЗОПАСНОГО ПОЛЬЗОВАНИЯ БАНКОВСКОЙ КАРТОЙ (ДЛЯ ДЕРЖАТЕЛЯ КАРТЫ, ЭМИТИРОВАННОЙ АО «ДАТАБАНК»)

Соблюдение рекомендаций, содержащихся в Правилах безопасного пользования банковской Картой платежных систем (для Держателя Карты, эмитированной АО «Датабанк») (далее – Правила безопасности карт), позволит обеспечить максимальную сохранность банковской Карты, ее реквизитов, ПИН-кода 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 с использованием Сервисов удаленного обслуживания Банка (через сеть Интернет).

1. ОБЩИЕ РЕКОМЕНДАЦИИ

1.1. В целях обеспечения защиты от несанкционированного доступа к Счету/Карте и сохранности средств необходимо соблюдать следующие обязательные правила:

- не допускать проведения операций с использованием Карты не Держателем Карты;
- при получении конверта с ПИН-кодом убедиться, что конверт не вскрыт;
- во время и после вскрытия конверта с ПИН-кодом обеспечить недоступность ПИН-кода третьим лицам;
- необходимо хранить Карту в недоступном для третьих лиц месте;
- запрещается хранить конверт с ПИН-кодом или записанный в том или ином виде ПИН-код вместе с Картой;
- запрещается записывать ПИН-код на Карте;
- если Держатель забыл ПИН-код, необходимо обратиться в Банк для замены Карты и получения нового ПИН-кода;
- запрещается сообщать ПИН-код третьим лицам (никто, даже работники Банка, не знают ПИН-код Клиента и НЕ ВПРАВЕ требовать от Держателя его назвать).
- никогда не сообщайте ПИН-код третьим лицам, в том числе родственникам, знакомым, работникам кредитной и/или иной организации, кассирам и лицам, помогающим Вам в использовании банковской Карты;
- необходимо регулярно проверять состояние Счета/Карты, даже если Карта не использовалась. Для получения информации о состоянии Счета можно использовать выписки по счету, SMS-информирование, уведомления Сервисов удаленного доступа Банка.

1.2. ПИН-код необходимо запомнить или в случае, если это является затруднительным, хранить его отдельно от Карты в неявном виде и недоступном для третьих лиц, в том числе родственников, месте.

1.3. 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.

1.4. 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 её утраты.

1.5. 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 во избежание её размагничивания.

1.6. Телефон Банка — эмитента банковской Карты (кредитной организации, выдавшей банковскую Карту) указан на оборотной стороне банковской Карты. Также необходимо всегда иметь при себе контактные телефоны Банка — эмитента банковской карты и номер банковской

Карты на других носителях информации: в записной книжке, мобильном телефоне и/или других носителях информации, но не рядом с записью о ПИН-коде.

1.7. С целью предотвращения неправомерных действий по снятию всей суммы денежных средств со Счета Карты целесообразно установить суточный лимит на сумму операций по банковской Карте и одновременно подключить электронную услугу оповещения о проведенных операциях (например, оповещение посредством SMS/push-уведомлений или иным способом – указываются Клиентом в Анкете-заявлении).

1.8. При получении просьбы, в том числе со стороны работника Банка, сообщить персональные данные или информацию о Карте (в том числе ПИН-код) не сообщайте их. Перезвоните в Банк — эмитент банковской Карты (кредитную организацию, выдавшую банковскую карту) и сообщите о данном факте.

ПОЖАЛУЙСТА, ЗАПОМНИТЕ! работники Банка (другой кредитной организации, любого Оператора денежных переводов), как и работники Платежной системы, НИКОГДА не запрашивают ПИН-код к Вашей Карте, реквизиты Счета для её использования.

1.9. Не рекомендуется отвечать на электронные письма, в которых от имени кредитной организации (в том числе Банка — эмитента банковской карты (кредитной организации, выдавшей банковскую Карту)) предлагается предоставить персональные данные. Не следуйте по «ссылкам», указанным в письмах (включая ссылки на сайт Банка), т.к. они могут вести на сайты-двойники.

1.10. В целях информационного взаимодействия с Банком — 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 Банке — эмитенте банковской Карты.

1.11. Помните, что в случае раскрытия ПИН-кода, персональных данных, утраты банковской Карты существует риск совершения неправомерных действий с денежными средствами по Вашему банковскому Счету со стороны третьих лиц.

1.12. В случае если имеются предположения о раскрытии ПИН-кода, персональных данных, позволяющих совершить неправомерные действия с Вашим банковским Счетом, а также, если банковская Карта была утрачена, необходимо немедленно обратиться в Банк — эмитент банковской Карты (кредитную организацию, выдавшую банковскую Карту) и следовать указаниям работника Банка.

До момента обращения в Банк — эмитент банковской Карты Вы несете риск, связанный с несанкционированным списанием денежных средств с Вашего банковского Счета. В соответствии с Договором (УДБО) между Вами-Клиентом и Банком — эмитентом банковской карты денежные средства, списанные с Вашего банковского Счета в результате несанкционированного использования Вашей банковской Карты до момента уведомления об этом Банка — эмитента банковской Карты, не возмещаются.

1.12. При получении Банком сообщения о возможности компрометации Карты (потери ее данных) Банк рекомендует Держателю Карты инициировать перевыпуск скомпрометированной Карты с целью минимизации рисков.

ВНИМАНИЕ! В случае устного или письменного отказа Держателя Карты от перевыпуска скомпрометированной Карты, Банк в дальнейшем не несет ответственности за несанкционированные операции по такой Карте и вправе не рассматривать претензии Клиента относительно возможного и/или действительного несанкционированного использования Карты третьими лицами.

2. РЕКОМЕНДАЦИИ ПРИ СОВЕРШЕНИИ ОПЕРАЦИЙ С КАРТОЙ В БАНКОМАТЕ

2.1. Осуществляйте операции с использованием банкоматов, установленных в безопасных местах (например, в государственных учреждениях, подразделениях банков, крупных торговых комплексах, гостиницах, аэропортах и т.п.).

2.2. Не используйте устройства, которые требуют ввода ПИН-кода для доступа в помещение, где расположен банкомат.

2.3. В случае если поблизости от банкомата находятся посторонние лица, следует выбрать более подходящее время для использования банкомата или воспользоваться другим банкоматом.

2.4. Перед использованием банкомата осмотрите его на наличие дополнительных устройств, не соответствующих его конструкции и расположенных в месте набора ПИН-кода и в месте (прорезь), предназначенном для приема Карт (например, наличие неровно установленной

клавиатуры набора ПИН-кода). В указанном случае воздержитесь от использования такого банкомата.

2.5. В случае если клавиатура или место для приема Карт банкомата оборудованы дополнительными устройствами, не соответствующими его конструкции, воздержитесь от использования Карты в данном банкомате и сообщите о своих подозрениях работникам Банка по телефону, указанному на банкомате.

2.6. Не применяйте физическую силу, чтобы вставить банковскую Карту в банкомат. Если банковская Карта не вставляется, воздержитесь от использования такого банкомата.

2.7. Набирайте ПИН-код таким образом, чтобы люди, находящиеся в непосредственной близости, не смогли его увидеть. При наборе ПИН-кода прикрывайте клавиатуру рукой.

2.8. 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 Карты.

2.9. После получения наличных денежных средств в банкомате следует пересчитать банкноты полистно, убедиться в том, что Карта была возвращена банкоматом, дождаться выдачи квитанции при ее запросе, затем положить их в сумку (кошелек, карман) и только после этого отходить от банкомата.

2.10. Следует сохранять распечатанные банкоматом квитанции для последующей сверки указанных в них сумм с выпиской по банковскому Счету Карты.

2.11. Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций с банковской Картой в банкоматах.

2.12. Если при проведении операций с банковской Картой в банкомате банкомат не возвращает Карту, следует позвонить в кредитную организацию по телефону, указанному на банкомате, и объяснить обстоятельства произошедшего, а также, следует обратиться в Банк — эмитент банковской Карты (кредитную организацию, выдавшую банковскую Карту), которая не была возвращена банкоматом, и далее следовать инструкциям работника Банка.

3. РЕКОМЕНДАЦИИ ПРИ ИСПОЛЬЗОВАНИИ КАРТЫ ДЛЯ БЕЗНАЛИЧНОЙ ОПЛАТЫ ТОВАРОВ И УСЛУГ

3.1. Не используйте банковские Карты в организациях торговли и услуг, не вызывающих доверия.

Держатель Карты самостоятельно определяет надежность торговой точки для предоставления информации по Карте.

3.2. 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.

3.3. При использовании банковской Карты для оплаты товаров и услуг кассир может потребовать от Держателя банковской Карты предоставить паспорт, подписать чек или ввести ПИН-код. Перед набором ПИН-кода 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 в чеке.

3.4. В случае если при попытке оплаты банковской Картой имела место «неуспешная» операция, следует сохранить один экземпляр выданного терминалом чека для последующей проверки на отсутствие указанной операции в выписке по банковскому счету.

4. РЕКОМЕНДАЦИИ ПРИ СОВЕРШЕНИИ ОПЕРАЦИЙ С БАНКОВСКОЙ КАРТОЙ ЧЕРЕЗ СЕТЬ ИНТЕРНЕТ

4.1. Не используйте ПИН-код при заказе товаров и услуг через сеть Интернет, а также по телефону/факсу.

4.2. Не сообщайте персональные данные или информацию о банковской(ом) Карте (Счете) через сеть Интернет, например ПИН-код, пароли доступа к ресурсам Банка, срок действия банковской Карты, кредитные лимиты, историю операций, персональные данные.

4.3. С целью предотвращения неправомерных действий по снятию всей суммы денежных средств со Счета Карты рекомендуется для оплаты покупок в сети Интернет использовать отдельную банковскую Карту - цифровую Карту Банка с предельным лимитом, предназначенную

только для указанной цели и не позволяющую проводить с ее использованием операции в организациях торговли и услуг.

4.4. Следует пользоваться интернет-сайтами только известных и проверенных организаций торговли и услуг.

4.5. Обязательно убедитесь в правильности адресов интернет-сайтов, к которым подключаетесь и с помощью которых собираетесь совершить покупки, т.к. похожие адреса могут использоваться для осуществления неправомерных действий.

4.6. 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).

4.7. 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.