# Памятка по информационной безопасности при использовании карточных продуктов АО «Кубаньторгбанк»

## Общие рекомендации

1. Никогда не сообщайте ПИН-код третьим лицам, в том числе родственникам, знакомым, сотрудникам кредитной организации, кассирам и лицам, помогающим Вам в использовании банковской карты.
2. ПИН-код необходимо запомнить или в случае, если это является затруднительным, хранить его отдельно от банковской карты.
3. Никогда ни при каких обстоятельствах не передавайте банковскую карту или ее реквизиты для использования третьим лицам, в том числе родственникам.
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 ее утраты.
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.
6. С целью предотвращения неправомерных действий по снятию денежных средств с банковского счета целесообразно установить ежедневный и/или ежемесячный лимит на сумму операций по банковской карте.
7. Если Вы обнаружили, что не работает мобильный телефон, используемый для получения сообщений от Банка (например, без видимых причин на длительное время пропала связь), незамедлительно обратитесь в Банк и заблокируйте банковскую карту.
8. Принимайте меры для предотвращения риска изготовления дубликата Вашей сим-карты:
   - пользуйтесь номером телефона, который оформлен лично на Вас,
   - не используйте анонимные сим-карты,
   - не передавайте мобильный телефон или сим-карту в пользование третьим лицам,
   - обратитесь к Вашему мобильному оператору для запрета выпуска дубликатов сим-карты, а также совершения действий с Вашей сим-картой на основании доверенности.
9. В случае подозрения на компрометацию банковской карты, например, если карта находилась или могла находиться в руках третьего лица, незамедлительно обратитесь в Банк и заблокируйте банковскую карту.
10. При получении просьбы, в том числе со стороны сотрудника кредитной организации, системы интерактивных голосовых ответов (IVR) или посредством SMS-сообщений, предоставить персональные данные или информацию о банковской карте (номер, срок действия, ПИН-код, код безопасности) не сообщайте их.
11. Не рекомендуется отвечать на электронные письма, в которых от имени кредитной организации (в том числе АО
12. «Кубаньторгбанк») предлагается предоставить персональные данные. Не следуйте по «ссылкам», указанным в письмах (включая ссылки на сайт кредитной организации), т.к. они могут вести на сайты-двойники.
13. Помните, что в случае раскрытия ПИН-кода, персональных данных, утраты банковской карты существует риск совершения неправомерных действий с денежными средствами на Вашем банковском счете со стороны третьих лиц.

## 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-кода 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-кода и в месте (прорезь), предназначенном для приема карт (например, наличие неровно установленной клавиатуры для набора ПИН-кода).
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. Наклейки на банкомате содержат торговые марки платежных систем и категорий банковских карт, которые принимаются к обслуживанию в данном устройстве. Используйте банкомат, на котором размещена информация, соответствующая Вашей банковской карте.
8. Рекомендуем последовательно выполнять команды, появляющиеся на экране банкомата в процессе совершения операции.
9. Набирайте ПИН-код таким образом, чтобы люди, находящиеся в непосредственной близости, не смогли его увидеть. При наборе ПИН-кода прикрывайте клавиатуру рукой.
10. 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.
11. По завершении операции следует незамедлительно забрать из банкомата банковскую карту, распечатанную квитанцию (чек) и денежные средства (при получении наличных средств).
12. Следует сохранять распечатанные банкоматом квитанции для последующей сверки указанных в них сумм с выпиской по банковскому счету.
13. Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций с банковской картой в банкоматах.
14. Если при проведении операций с банковской картой банкомат не возвращает банковскую карту, следует позвонить в кредитную организацию по телефону, указанному на банкомате, и объяснить обстоятельства произошедшего.

## 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-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 на чеке.
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.

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

1. Не используйте ПИН-код 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-код, пароли доступа к системе ДБО, срок действия банковской карты, платежный лимит, историю операций, персональные данные.
3. Совершение операций через интернет-сайты, которые сертифицированы международной платежной системой MasterCard Worldwide на технологию «Mastercard SecureCode», необходимо ввести одноразовый пароль (предоставляется в виде СМС-сообщения/ Push-уведомления на мобильный телефон).
4. Следует пользоваться интернет-сайтами только известных и проверенных организаций торговли и услуг.
5. 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.
6. Рекомендуется совершать покупки только со своего компьютера/ мобильного устройства 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/ мобильное устройство 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.