Приложение 7
к Условиям дистанционного банковского обслуживания
в ООО «Крона-Банк» с использованием электронной системы «Интернет-Банк»

Памятка по использованию Мобильного приложения

1. При потере мобильного устройства/смене номера телефона обязательно сообщите об этом в Банк.

2. Клиент должен использовать процедуру аутентификации доступа к мобильному устройству (ввод пароля для разблокировки мобильного устройства), прежде чем приступить к совершению операций через Мобильное приложение, если иной способ доступа не избран самим Клиентом.

3. Используйте только официальные приложения Банка, доступные в официальных репозиториях производителей мобильных платформ.

4. Своевременно устанавливайте доступные обновления операционной системы и приложений на Ваш телефон.

5. Портативное устройство не должно быть подвергнуто операциям повышения привилегий / взлома операционной системы.

6. Используйте антивирус для мобильного устройства, своевременно устанавливайте на него обновления вирусных баз.

7. Не переходите по ссылкам и не устанавливайте приложения/обновления безопасности, пришедшие по СМС/электронной почте, в том числе от имени Банка.

8. Установите парольную защиту на мобильном устройстве, данная возможность доступна для любых современных мобильных устройств.

9. Установленный Цифровой код для входа в Мобильное приложение должен быть сложен для угадывания (отличаться от последовательности одинаковых символов, даты или года рождения Клиента и т.д.).

10. Клиент никогда и никому не должен сообщать Цифровой код для входа в Мобильное приложение.

11. Клиент, используя мобильное устройство, с которого получает доступ к Мобильному приложению, осуществляет избирательную навигацию в сети Интернет, и старается не посещать неизвестные ему сайты, устанавливать сомнительные приложения.

12. Клиент обязуется не подключать мобильное устройство к компьютерам, безопасность которых (обеспечение доверенных сред, лишенных удаленного управления и установленных / запущенных вредоносных программ) он не может гарантировать.

13. Клиент обязуется не модифицировать или изменять Мобильное приложение, устанавливать приложение только из официальных хранилищ.

14. Клиент понимает и подтверждает, что в Банк отправляются сведения о его геолокации.

15. Никогда не передавайте свое мобильное устройство и/или sim-карту третьим лицам.

16. Клиент, подключая опцию «совместная аналитика», дает поручение Банку передавать информацию об операциях по Счетам третьему лицу, указанному Клиентом при подключении вышеуказанной опции.

17. В случае если вы (Клиент) устанавливаете возможность просмотра информации в Мобильном приложении системы «Интернет-Банк» без ввода Цифрового кода, вы осознаете возможность реализации следующих рисков:

- в случае утери/кражи или выбытия мобильного устройства по иному основанию помимо воли Клиента, третьи лица могут получить доступ к следующей информации: о номере счета/счетов Клиента, об остатках и движении денежных средств по счету/счетам, фамилии, имени, отчества владельца счета, наименование организации, которой принадлежит счет.

• в целях минимизации возможности реализации указанных в настоящем пункте рисков установите пароль для разблокировки мобильного устройства (в случае наличия технической возможности). В случае отсутствия такой возможности Банк рекомендует не пользоваться услугой, позволяющей отменить Цифровой код для входа в Мобильное приложение системы «Интернет-Банк»» с целью просмотра информации.

• независимо от того, используете ли вы пароль для разблокировки мобильного устройства, риск возникновения негативных последствий, описанных в настоящем пункте, увеличивается в сравнении с тем, если бы вы постоянно использовали цифровой код в мобильном приложении системы «Интернет-Банк» для совершения любых действий, в том числе просмотра информации.

18. В случае установки Виджета Клиентом, использующим Мобильное приложение, Клиент осознает, что возможна реализация следующих рисков:

• в случае передачи Клиентом, утери/кражи или выбытия мобильного устройства по иному основанию помимо воли Клиента третьи лица могут получить доступ к следующей информации:

- текущий баланс Счета (-ов);

- о трех последних операциях, совершенных по Счету (-ам) Клиента;

В целях минимизации возможности реализации указанных в настоящем пункте рисков установите пароль для разблокировки мобильного устройства (в случае наличия технической возможности ограничения доступа к информации Виджета). В случае отсутствия такой возможности Банк рекомендует не пользоваться вышеуказанной опцией. Факт использования Виджета несет повышенный риск возникновения негативных последствий, описанных в настоящем пункте, в сравнении с тем, если бы Вы постоянно использовали исключительно Мобильное приложение для просмотра информации.

19. В случае использования Клиентом – пользователем Мобильного приложения, Клиент осознает, что возможна реализация следующих рисков:

• в случае передачи Клиентом, утери/кражи или выбытия мобильного устройства по иному основанию помимо воли Клиента третьи лица могут получить доступ к следующей информации:

- о текущем балансе Счета(-ов);

В целях минимизации возможности реализации указанных в настоящем пункте рисков установите пароль для разблокировки мобильного устройства.

20. Банк не отвечает за убытки Клиента, возникшие в результате:

• внесения Клиентом или третьими лицами изменений в программное обеспечение мобильного устройства, компьютера или иного устройства, обеспечивающего доступ в Мобильное приложение, а также в результате наличия «вирусов» и иных вредоносных программ в указанных устройствах и программном обеспечении, используемом Клиентом для доступа в Мобильное приложение.

• неправильного указания платежных реквизитов в распоряжениях на осуществление платежа, а также иной информации, необходимой для оказания Услуг.