1. Anlayışlar və təyinlər

* Sistem – Mobil qurğuya qabaqcadan quraşdırılmış, barəsində Servis-provayderin müstəsna hüquqlara malik olduğu, özlüyündə Ödəniş xidmətlərinin göstərilməsi üçün Mobil qurğulara əlavə təmsil edən proqram təminatı.

* Servis-provayder – Müştərinin, Ödəniş xidmətlərinin təqdim edilməsi haqqında müqavilə bağladığı, Mobil qurğunun istehsalçısı olan şirkət.

* Bank — «Unibank» Açıq Səhmdar Cəmiyyəti

* Müqavilə — Kompleks bank xidməti şərtləri.

* Müştəri — Bankla müqavilə bağlamış fiziki şəxs.

* Toxunuşsuz ödəniş – toxunuşsuz hesablama qurğusunda Rəqəmsal kartdan istifadə etməklə yerinə yetirilmiş ödəniş.

* Autentifikasiya verilənləri – Müştərinin avtorizasiya üçün parolu (biometrik verilənlər (barmaq izinə görə avtorizasiya, sifətin tanınması) də daxil olmaqla, lakin onlarla məhdudlaşmayaraq), FEN-kodu, qrafik açarı, həmçinin Sistemə daxil olmaq üçün istifadə edilən digər verilənlər. Autentifikasiya verilənləri Müştərinin öz əli ilə atdığı imzanın analoqudurlar.

* Rəqəmsal kart – Müştərinin, Sistemdə istifadə üçün seçdiyi və qeydiyyatdan keçirdiyi kart.

* Mobil qurğu – naqilsiz ödəniş qurğusu.

2. Başlıca müddəalar

2.1. Bu sənəddə, Bankın istənilən Rəqəmsal kartlarından Sistemdə istifadə edilməsini tənzimləyən şərtlər yer almışdır. Bu Şərtlər, Kart müqaviləsinə və cari Əlavədəki lisenziya sazişinə əlavədirlər.

2.2. Bu Şərtlər, Bankla Müştəri arasında münasibətlərdə Müştərinin Rəqəmsal kart ilə giriş və ondan istifadə qaydalarını müəyyən edir.

3. İş prinsipi

3.1. Ödənişlərin həyata keçirilməsi

3.1.1. Sistem, Müştərinin satış məntəqələrindəki toxunuşsuz terminallarda toxunuşsuz ödənişləri yerinə yetirə bilməsi üçün, Müştərinin Mobil qurğusunda Kartın Virtual təsvirini yaratmaq imkanı verir;

3.1.2. Müştəri Kartı, onu öz kartlarının arasından seçərək, elektron pul qabında qeydiyyatdan keçirir. Kartın müvəffəqiyyətli verifikasiyasından sonra, Sistem Rəqəmsal kartı formalaşdırır və Sistemdə onun Virtual təsvirini formalaşdırır.

3.1.3. Müştəri, Rəqəmsal kartın köməyi ilə Bank tərəfindən müəyyən edilmiş limitdən yuxarı ödənişin yerinə yetirilməsi üçün, Rəqəmsal kartın razılığa əsaslanan Virtual təsvirini seçərək və Mobil qurğunu

satış məntəqəsindəki toxunuşsuz ödəniş terminalı və yaxud hesablayışı qurğu ilə yanaşı yerləşdirərək, Autentifikasiya verilənlərini daxil etmək yolu ilə ödənişi təsdiq edir.

3.1.4. Müştəri, Rəqəmsal kartın köməyi ilə Bank tərəfindən müəyyən edilmiş limitdən aşağı ödənişin yerinə yetirilməsi üçün, Rəqəmsal kartın razılığa əsaslanan Virtual təsvirini seçərək və Mobil qurğunu satış məntəqəsindəki toxunuşsuz ödəniş terminalı və yaxud hesablayışı qurğu ilə yanaşı yerləşdirərək, Autentifikasiya verilənlərini daxil etmək yolu ilə ödənişi təsdiq edir.

3.2. İnformasiyanın və ödənişlərin nəzərdən keçirilməsi

3.2.1. Sistem Müştəriyə, Rəqəmsal kart vasitəsi ilə bundan əvvəl yerinə yetirilmiş əməliyyatlar (alışın tarixi, məbləği, satıcının adı) haqqında informasiyaya giriş təqdim edir.

3.2.2. Sistem, Sistemin köməyi olmadan yerinə yetirilmiş əməliyyatlar haqqında informasiya təqdim edə bilmir.

3.3. Müştərinin hüquq və öhdəlikləri

3.3.1. Müştəri, Sistemdə qeydiyyatdan keçənə kimi, Sistemdə ancaq Müştərinin biometrik verilənlərinin (barmaq izinə görə avtorizasiya, sifətin tanınması) qeydiyyata alındığına, Kartdan istifadə edilməklə əməliyyatlar üzrə sövdələşmələrin təsdiq edilməsi zamanı ancaq bu barmaq izlərinin nəzərə alınacağına əmin olmalıdır. Əgər Müştəri, Mobil qurğuda avtorizasiya üçün və yaxud barmaq izinə görə daxil olmaq üçün və ya Müştərinin Mobil qurğusunda əməliyyatların yerinə yetirilməsi üçün başqa şəxsin barmaq izlərindən (və yaxud Autentifikasiya verilənlərindən) istifadə edirsə, onlar Müştərinin barmaq izləri hesab ediləcəklər.

3.3.2. Müştəri öz Autentifikasiya verilənlərini üçüncü şəxslər üçün əlçatmaz yerdə saxlamalıdır.

3.3.3. Müştəri, Autentifikasiya verilənlərinin və ya Rəqəmsal kartın verilənlərinin itirildiyi və/və ya kompрometasiya olunduğu halda, dərhal bu barədə Bankı məlumatlandırmağa borcludur .

3.3.4. Autentifikasiya verilənlərinin və ya Rəqəmsal kartın verilənlərinin itirildiyi və/və yaxud kompрometasiya olunduğu barədə Müştəri tərəfindən Bankın məlumatlandırılmadığı və/və ya vaxtında məlumatlandırılmadığı halda, Bank Müştərinin mümkün olan itkiləri üçün məsuliyyət daşımır.

3.3.5. Müştərinin Rəqəmsal kartının və Autentifikasiya verilənlərinin köməyi ilə həyata keçirilmiş alışlar və ya digər əməliyyatlar Müştərinin əməliyyatları hesab edilirlər.

3.3.6. Rəqəmsal kartın yaradılması üçün, Müştərinin adına açılmış, ləğv edilməmiş və ya bloka alınmamış istənilən kartdan istifadə etmək olar.

3.3.7. Müştəri istənilən vaxt, Sistemdən Rəqəmsal kartı siməklə, Ödəniş xidmətlərindən imtina etmək hüququna malikdir.

3.4. Bankın hüquq və öhdəlikləri

3.4.1. Müştəriyə Sistemdə Kartın qeydiyyata alınmasında və Rəqəmsal kartın yaradılmasında imtina etmək.

3.4.2. Rəqəmsal kartın hərəkətini və ondan Sistemdə istifadə edilməsi imkanını bloka almaq, Kartın / Rəqəmsal kartın Sistemdən çıxarılması haqqında sərəncam vermək və bunun üçün bütün zəruri tədbirlər görmək:

3.4.2.1. Müştəri tərəfindən, bu Şərtlərlə nəzərdə tutulmuş öhdəliklər yerinə yetirilmədikdə və yaxud lazımi qaydada yerinə yetirilmədikdə;

3.4.2.2. Rəqəmsal kartdan və/və ya Kartdan sanksiya verilməmiş istifadə edilməsi barədə şübhələr olduqda.

3.4.3. Limiti, Müştərinin Autentifikasiya verilənlərinin daxil edilməsini tələb edən məbləğdə, dəyişmək.

3.4.4. Bank, Müştərinin Rəqəmsal kartdan istifadə məsələləri üzrə informasiya dəstəyini 117 nömrəli telefonla təmin etməyə borcludur.

4. Məxfilik və təhlükəsizlik

4.1. Şəxsi məlumatlar

4.1.1. Müştəri bununla tanış olur və razılaşır ki, Bank, aşağıdakıları təmin etmək üçün, texniki, şəxsi verilənlərin və onlarla bağlı informasiyanın toplanmasını, emalını və ondan istifadə edilməsini həyata keçirmək hüququna malikdir:

4.1.2. Bankın məhsullarının, xidmətlərinin yenilənməsi və təkmilləşdirilməsi;

4.1.3. Göstərilən xidmətlərin təhlükəsizliyinin yüksəldilməsi;

4.1.4. Möhtəkirliyin qarşısının alınması;

4.2. Digər şəxslər tərəfindən toplanan informasiya.

4.2.1. Bank, Sistemin və yaxud Servis-provayderin digər kənar təchizatçısının xidmətləri üçün məsuliyyət daşımır. Beləliklə, Müştəri tərəfindən Rəqəmsal kartdan və ya Sistemdən istifadə olunması zamanı Servis-provayderin topladığı istənilən informasiya Servis-provayderin Şərtləri ilə və üçüncü tərəflərlə bağlanmış Müqavilələrlə tənzim edilir, lakin bu Şərtlərlə, Müqavilə ilə və Bankın məxfilik siyasəti ilə tənzim olunmurlar.

4.3. Müştərinin Mobil qurğusunun itirilməsi, oğurlanması və ya ondan sanksiya verilməmiş istifa edilməsi.

4.3.2. Autentifikasiya verilənlərinin komprometasiya olunması halında və yaxud komprometasiya olunmasına şübhənin olduğu halda, Müştəri dərhal özünün şəxsi təhlükəsizlik məlumatlarını, Autentifikasiya verilənlərini dəyişməli və, Rəqəmsal kartdan və ya şəxsi informasiyadan istənilən sanksiya verilməmiş istifadədən uzaq olmaq üçün, Mobil qurğuda ancaq icazə verilmiş barmaq izlərinin qeydiyyata alındığına əmin olmalıdır.

4.3.3. Yeni Mobil qurğunun alınması zamanı Müştəri, dəyişdirilən mobil qurğuda bütün Rəqəmsal kartların, digər şəxsi informasiyanın silindiyinə əmin olmalıdır. Bunun üçün Müştəri Banka 117 nömrəli telefonla, Rəqəmsal kartların silinməsi haqqında sərəncamla müraciət edə bilər.

4.3.4. Müştəri, istənilən təhqiqatların aparılması zamanı Banka dəstək verməli və möhtəkirliyin və kartların kompрometasiyasının qarşısını ala biləcək digər tədbirlərdən istifadə etməlidir.

4.4. Sistemin parollarının, digər Autentifikasiya verilənlərinin və Kartların (Rəqəmsal kart qismində seçilmişlərin) mühafizəsi.

4.4.1. Müştəri, şəxsi təhlükəsizlik məlumatlarının və Autentifikasiya məlumatının məxfiliyini təmin etməlidir. Müştəri, onların qorunub saxlanmasını, habelə Mobil qurğunun qorunub saxlanmasını, Bank kartlarının və Müştərinin şəxsiyyətini təsdiq edən digər məlumatların, nömrələrin və parolların qorunub saxlanmasını təmin etdiyi qaydada, təmin etməlidir.

4.4.2. Bank, Rəqəmsal kartın təhlükəsizliyi üzrə məlumatların, Müştəri tərəfindən istifadə olunan məlumatlardan ayrı saxlanılmasını təkidlə tövsiyə edir. Bank kartlarını Mobil qurğu ilə bir yerdə saxlamamalı.

4.4.3. Bank, Mobil qurğunun blokdan çıxarılması vasitəsi kimi qrafik açardan istifadə edilməsini tövsiyə etmir.

4.4.4 Bank, Servis-provayderlə razılaşdırılmadan, proqram təminatının sanksiya verilməmiş quraşdırılması üçün qurğunun sındırldığı təqdirdə, təhlükəsizliyi təmin etmir.

4.4.5. Bank, işləyib hazırlayanın parametrlərinin Müştərinin Mobil qurğusuna daxil edilməsini tövsiyə etmir.

4.4.6. Müştərinin kartı sistemə əlavə etməsi barəsində bildirişi aldıqdan sonra, bu şərtlə ki, Müştəri bu cür qeydiyyatı yerinə yetirməmiş olsun, və yaxud Mobil qurğuda və ya Kart üzrə çıxarışda Müştərinin tanımadığı hər hansı bir əməliyyat olduqda, dərhal 117 nömrəsi ilə Banka müraciət edin.

---

1. Terms and definitions

* The System is a software installed on the Mobile Device, under the exclusive rights owned by the Service Provider, which software is a mobile device application supporting the Payment Services.

* The Service Provider is a manufacturer company of the Mobile Device with which the Customer has concluded an agreement about the provision of the Payment Services.

* The Bank – Unibank Open Joint-Stock Company.

* The Agreement – the conditions of the integrated banking service.

* The Customer – a natural person who has concluded the Agreement with the Bank.

* The Proximity Payment – a payment made by means of the Digital Card at a contactless reader device.

* The Authentication Data – the Customer password used for authorisation (including, but not limited to, the biometric data (fingerprint authorisation, face recognition), a PIN code, a graphic key and the

other data used to gain access to the System. The Authentication Data are an analogue of the written signature made by the Customer.

* The Digital Card – a card that the Customer has chosen and had had registered for the use in the System.

* The Mobile Device – a wireless payment device.

2. The Basic Provisions

2.1. The present document contains the conditions regulating the use of all Digital Cards of the Bank in the System. The present Conditions are an appendix to the Card Agreement and the Licence Agreement attached hereto.

2.2. The present Conditions set the rules of access and use of the Customer's Digital Card in the relationship between the Bank and the Customer.

3. Modus Operandi

3.1. Making the Payments

3.1.1. The System permits creation of a Virtual Concept of the Card on the Customer's Mobile Device for the Customer to be able to make proximity payments at contactless terminals at points of sales;

3.1.2. The Customer shall register the Card in the e-wallet by having selected the former from amongst his/her cards. Once the Card has been verified successfully, the System will form the Digital Card and form its Virtual Concept within the System.

3.1.3. To make a payment in excess of the limit determined by the Bank using the Digital Card, the Customer will select the appropriate Virtual Concept of the Digital Card setting it as one by default and, having positioned the Mobile Device next to the contactless payment terminal at a point of sales or next to a reader device, will confirm the payment by entering the Authentication Data.

3.1.4. To make a payment below the limit determined by the Bank using the Digital Card, the Customer will select the appropriate Virtual Concept of the Digital Card setting it as one by default and shall confirm the payment by positioning the Mobile Device next to the contactless payment terminal at a point of sales or next to a reader device.

3.2. Viewing Information and Payments

3.2.1. The System gives the Customer access to the Digital Card information about previous transactions made with it, such as the date and amount of purchase and vendor name.

3.2.2. The System cannot display information about transactions not conducted by means of the System.

3.3. The Rights and Obligations of the Customer

3.3.1. The Customer must make certain, before the registration in the System, that only the biometrics of the Customer (fingerprints, face recognition inputs) are registered with the System and only such fingerprints will be taken into account to confirm the Card transactions. If fingerprints (or the Authentication Data) of another person are used for either the authorisation on the Mobile Device or for the Access, such fingerprints will be deemed the fingerprints of the Customer.

3.3.2. The Customer must store his/her Authentication Data in a place beyond the third-party reach.

3.3.3. In the event of the compromising of the Authentication Data and/or the Digital Card data, the Customer must notify the Bank accordingly without any delay.

3.3.4. Should the Customer fail to notify and/or make a belated notification to the Bank of the loss of the Authentication Data and/or the compromise of the Digital Card details, the Bank shall not be liable for any possible loss of the Customer.

3.3.5. Purchases and other transactions conducted by means of the Digital Card and the Authentication Data of the Customer shall be deemed the Customer transactions.

3.3.6. The Customer may use any Card that is opened in the Customer's name and is not either terminated or blocked for the generation of the Customer Card.

3.3.7. The Customer has the right to decline to use the Payment Services and delete the Digital Card from the System at any time.

3.4. The Rights and Obligations of the Bank

3.4.1. To deny the Customer a Card registration and a Digital Card generation within the System.

3.4.2. To block the Digital Card or make it unusable within the System, to order to recall the Card/Digital Card and make every appropriate arrangement to this end:

3.4.2.1. If the Customer has failed or ill-performed his/her obligations subject hereto;

3.4.2.2. If a doubt is entertained as to any unauthorised use of the Digital Card and/or the Card.

3.4.3. To modify the payment limit requiring the input of the Customer's Authentication Data.

3.4.4. The Bank must provide the information support to the Customer about the use and usage of the Digital Card at the extension number 117

4. Confidentiality and Security

4.1. Personal Information

4.1.1. The Customer is informed of, and agrees with that the Bank shall have the right to collect, process and use technical and personal data and related information for the following purposes:

4.1.2. Upgrading and improving the products and services of the Bank;

4.1.3. Making the services provided safer;

4.1.4. Avoidance of fraudulent activities;

4.2. Information Collected by Other Parties

4.2.1. The Bank shall not be responsible for the services of the System or of an outside Service Provider. Consequently, any information that the Service Provider is or may be collecting when the Customer uses the Digital Card or the System is regulated by the Conditions of the Service Provider and the Third-Party Agreements, and is not governed by the present Conditions, the Agreement and the Confidentiality Policy of the Bank.

4.3. Loss, theft or unauthorised use of the Mobile Device of the Customer

4.3.2. In the event of a compromise or a suspected compromise of the Authentication Data the Customer must change the personal security data and the Authentication Data immediately and make certain that only the permitted fingerprints are registered on the Mobile Device for the avoidance of any unauthorised use of either the Digital Card or of the personal information.

4.3.3. On acquiring a new Mobile Device, the Customer must make certain that all the Digital Cards and other personal information are deleted from the former Mobile Device. To this end, the Customer may call the Bank at 117 to instruct it to delete the said Digital Cards.

4.3.4. The Customer must assist the Bank in any investigation and take steps to prevent fraudulent and other undesirable activities in order to discourage a compromise of the Card.

4.4. Protection of the System passwords, other Authentication Data and Cards (chosen for the employment as Digital Cards)

4.4.1. The Customer must keep the personal security and Authentication data т confidential. The Customer must keep them and the Mobile Device intact in the same way in which the Bank Cards and other data, numbers and passwords attesting to the identification of the Customer are kept intact.

4.4.2. The Bank recommends insistently that the Digital Card security data should be stored separately from the data used by the Customer and that the physical Bank Cards should not be stored together with the Mobile Device.

4.4.3. The Bank does not recommend the use of a graphical key as a means of unblocking the Mobile Device.

4.4.4. The Bank does not recommend security if a device has been hacked for the access for unauthorised software installation without an accommodation reached with the Service Provider.

4.4.5. The Bank does not recommend the input of the Developer Parameters in the Customer’s Mobile Device.

4.4.6. On receiving the information that the Customer has added a card to the System and providing that the Customer has not made such a registration or where there are some transactions that the Customer did not acknowledge on the Mobile Device or in the Card statement, please, call the Bank at 117 immediately.

---

1. Термины и определения

* Система - программное обеспечение, предустановленное в Мобильное устройство, исключительные права на которое принадлежат Сервис-провайдеру, представляющее собой приложение для Мобильных устройств, позволяющее оказывать Платежные услуги.

* Сервис-провайдер – компания, являющаяся производителем Мобильного устройства, с которым Клиент заключил договор о предоставлении Платежных услуг.

* Банк — Открыток Акционерное общество «Unibank»

* Договор — Условия комплексного банковского обслуживания.

* Клиент — физическое лицо, заключившее с Банком Договор.

* Бесконтактный платеж - платеж, произведенный при помощи использования Цифровой карты в бесконтактном считывающем устройстве.

* Аутентификационные данные - пароль Клиента для авторизации (включая, но не ограничиваясь биометрическими данными (авторизация по отпечатку пальца, распознаванию лица), ПИН-код, графический ключ, а также другие данные, используемые для доступа в Систему. Аутентификационные данные являются аналогом собственноручной подписи Клиента.

* Цифровая карта – Карта, которую Клиент выбрал и зарегистрировал для использования в Системе.

* Мобильное устройство - беспроводное платежное устройство.

2. Основные положения

2.1. В настоящем документе содержатся условия, регулирующие использование любых Цифровых карт Банка в Системе. Настоящие Условия являются дополнением к карточному договору и лицензионному соглашению в текущем приложении.

2.2. Настоящие Условия устанавливают правила доступа и использования Цифровой карты Клиента в отношениях между Банком и Клиентом.

3. Принцип работы

3.1. Осуществление платежей

3.1.1. Система позволяет создавать Виртуальное представление Карты на Мобильном устройстве Клиента, чтобы Клиент мог осуществлять бесконтактные платежи на бесконтактных терминалах в пунктах продаж;

3.1.2. Клиент регистрирует Карту в электронном кошельке, выбрав ее из списка своих карт. После успешной верификации Карты, Система формирует Цифровую карту и формирует ее Виртуальное представление в Системе.

3.1.3. Для осуществления оплаты на сумму выше лимита, установленного Банком с помощью Цифровой карты, Клиент, выбрав соответствующее Виртуальное представление Цифровой карты по умолчанию и разместив Мобильное устройство рядом с бесконтактным платежным терминалом в пункте продаж или считывающим устройством, Клиент подтверждает оплату путем ввода Аутентификационных данных.

3.1.4. Для осуществления оплаты на сумму ниже лимита, установленного Банком с помощью Цифровой карты, Клиент, выбрав соответствующее Виртуальное представление Цифровой карты по умолчанию, подтверждает оплату, разместив Мобильное устройство рядом с бесконтактным платежным терминалом в пункте продаж или считывающим устройством.

3.2. Просмотр информации и платежей

3.2.1. Система предоставляет Клиенту доступ к информации по Цифровой карте о предыдущих операциях, совершенных этой Цифровой картой: дата, сумма покупки, наименование продавца.

3.2.2. Система не может предоставить информацию по операциям, совершенными не с помощью Системы.

3.3. Права и обязанности Клиента

3.3.1. До регистрации в Системе Клиент обязан убедиться, что в Системе зарегистрирована только биометрия Клиента (отпечатки пальцев, распознавание лиц), только такие отпечатки пальцев будут учитываться при подтверждении сделок по операциям с использованием Карты. Если для авторизации в Мобильном устройстве или для Входа по отпечатку пальца, или совершения операций на Мобильном устройстве Клиента используют отпечатки пальцев (или Аутентификационные данные) другого лица, они будут считаться отпечатками пальцев Клиента.

3.3.2. Клиент обязан обеспечить хранение своих Аутентификационных данных в недоступном для третьих лиц месте.

3.3.3. В случае компрометации Аутентификационных данных и/или данных Цифровой карты, Клиент обязан незамедлительно уведомить об этом Банк.

3.3.4. В случае неуведомления и/или несвоевременного уведомления Клиентом Банка об утрате Аутентификационных данных и/или компрометации реквизитов Цифровой карты, Банк не несет ответственности за возможные убытки Клиента.

3.3.5. Покупки или другие операции, совершенные при помощи Цифровой карты и Аутентификационных данных Клиента, считаются операциями Клиента.

3.3.6. Использовать любую Карту, открытую на имя Клиента, не являющейся аннулированной или заблокированной, для создания Цифровой карты.

3.3.7. Клиент вправе в любое время отказаться от использования Платежных услуг, удалив Цифровую карту из Системы.

3.4. Права и обязанности Банка

3.4.1. Отказать Клиенту в регистрации Карты и создания Цифровой карты в Системе.

3.4.2. Блокировать действие Цифровой карты или возможность её использования в Системе, дать распоряжение об изъятии Карты / Цифровой карты и принимать для этого все необходимые меры:

3.4.2.1. в случае неисполнения или ненадлежащего исполнения Клиентом обязательств, предусмотренных настоящими Условиями;

3.4.2.2. в случае подозрений на несанкционированное использование Цифровой карты и/или Карты.

3.4.3. Изменять лимит на сумму оплат, требующих ввод Аутентификационных данных Клиента.

3.4.4. Банк обязан обеспечить информационную поддержку Клиента по вопросам использования Цифровой карты по телефону: 117

4. Конфиденциальность и безопасность

4.1. Личная информация

4.1.1. Клиент ознакомлен и соглашается, что Банк вправе осуществлять сбор, обработку и использование технических, личных данных и связанной с ними информации, чтобы обеспечивать:

4.1.2. обновление и усовершенствование продуктов, услуг Банка;

4.1.3. повышение безопасности оказываемых услуг;

4.1.4. предотвращение мошенничества;

4.2. Информация, собираемая другими лицами

4.2.1. Банк не несет ответственности за услуги Системы или другого стороннего поставщика Сервис-провайдера. Таким образом, любая информация, которую собирает Сервис-провайдер при использовании Клиентом Цифровой карты или Системы, регулируется Условиями Сервис-провайдера и Договорами с третьими сторонами, но не регулируется настоящими Условиями, Договором и Политикой конфиденциальности Банка.

4.3. Потеря, кража или несанкционированное использование Мобильного устройства Клиента

4.3.2. В случае компрометации или подозрений на компрометацию Аутентификационных данных, Клиент обязан незамедлительно изменить сведения личной безопасности, Аутентификационные

данные и убедиться, что в Мобильном устройстве зарегистрированы только разрешенные отпечатки пальцев во избежание любого несанкционированного использования Цифровой карты или личной информации.

4.3.3. При получении нового Мобильного устройства Клиент обязан убедиться, что стерты все Цифровые карты, иная личная информация в замененном мобильном устройстве. Для этого Клиент может обратиться в Банк по телефону 117 с распоряжением об удалении Цифровых карт.

4.3.4. Клиент обязан оказывать содействие Банку при проведении любых расследований и использовать меры для предотвращения мошенничества или иные меры, которые могут предотвратить компрометацию Карт.

4.4. Защита паролей Системы, иных Аутентификационных данных и Карт (которые выбраны для использования в качестве Цифровых карт).

4.4.1. Клиент обязан обеспечивать конфиденциальность сведений личной безопасности и Аутентификационных данных. Клиент обязан обеспечивать их сохранность, а также сохранность Мобильного устройства таким же образом, как обеспечивается сохранность банковских Карт и иных сведений, номеров и паролей, подтверждающих личность Клиента.

4.4.2. Банк настоятельно рекомендует сохранять сведения по безопасности Цифровой карты отдельно от сведений, используемых Клиентом. Не хранить физические банковские Карты с Мобильным устройством.

4.4.3. Банк не рекомендует использование графического ключа в качестве средства разблокировки Мобильного устройства.

4.4.4 Банк не гарантирует безопасность, если устройство было взломано для получения доступа несанкционированной установки программного обеспечения без согласования с Сервис-провайдером.

4.4.5. Банк не рекомендует включать Параметры разработчика на Мобильном устройстве Клиента.

4.4.6. При получении уведомления о том, что Клиент добавил карту в систему, при условии, что Клиент не осуществлял такой регистрации, либо при наличии каких-либо операций, которые Клиент не признал на Мобильном устройстве или в выписке по Карте, незамедлительно обратитесь в Банк по телефону 117.