

მობილური გადახდების სისტემაში საბანკო ბარათების გამოყენების წესები და პირობები

1. ტერმინები და განმარტებები

თითოეულ ტერმინს აქვს ერთი და იგივე მნიშვნელობა მიუხედავად იმისა, “პირობების” რომელი ადგილზე გვხვდება, ასევე, მხოლოდითის აღმნიშვნელი სიტყვები მოიცავს მრავლობითსაც და პირიქით.

* “მომსახურების გამწევი” * ნებისმიერი იურიდიული პირი, რომელიც წარმოადგენს მობილური ტერმინარის ვენდორს და რომელთანაც კლიენტს გაფორმებული აქვს ხელშეკრულება გადახდების მომსახურების გამწევის შესახებ.

* “სისტემა” – მობილურ ტერმინარში დაყენებული პროგრამული უზრუნველყოფა, რომელიც ექსპლუატირებული უფლებებიც ეკუთვნის “მომსახურების გამწევს”, აღნიშნული წარმოადგენს აპლიკაციას, რომელიც მობილურ ტერმინარებს აძლევს ანგარიშსწორების მომსახურების გამწევის შესაძლებლობას.

* “მომსახურების გამწევის პირობები” – სადოკუმენტო ხელშეკრულება პროგრამული უზრუნველყოფისა და მომსახურების გამწევის სხვა დამატებითი პირობების შესახებ, რომელიც გაფორმებულია “კლიენტსა” და მომსახურების გამწევს შორის.

* “ბანკი” – სააქციო საზოგადოება “თიბისი ბანკი. 0102, #7 მარჯანიშვილის ქ, თბილისი, საქართველო, ს/კ: 204854595

* “კონტრაქტი” – კომპლექსური საბანკო მომსახურების პირობები.

* “კლიენტი” – ფიზიკური პირი, ვინც ხელი მოაწერა ხელშეკრულებას “ბანკთან.”

* “უკონტაქტო ანგარიშსწორება” – უკონტაქტო წამკითხველ მონაცემთაში ციფრული ბარათის გამოყენებით განხორციელებული ანგარიშსწორება.

* “აუთენტიფიკაციის მონაცემები” – კლიენტის პაროლი მობილურ აპლიკაციაში ავტორიზაციის მიზნით (მათ შორის და არა მხოლოდ, ბიომეტრიული მონაცემები (ავტორიზაცია თითის ანაბეჭდით (Touch ID), იდენტიფიკაცია სახით (დაცული აუთენტიფიკაცია)) ან “მომსახურების გამწევი“-ს მიერ მოწოდებული სხვა ახალი ტექნოლოგია, რომელიც დაყენებულია “მომსახურების გამწევის პირობების” შესაბამისად, პინ-კოდი, აგრეთვე სხვა მონაცემები, რომლებიც გამოყენება სისტემაში შესასვლელად. აუთენტიფიკაციის მონაცემები არის “კლიენტის” საკუთარი ხელმოწერის ანალოგი.

* “ციფრული ბარათი” – “სისტემაში” გამოყენების მიზნით “კლიენტის” მიერ შეჩვენებული და რეგისტრირებული ბარათი.

* “ბარათი” – საბანკო პლასტიკური ბარათით მომსახურება გურისხმობს მომხმარებლის ან მის მიერ წერილობით შეტყობინებულ ნებისმიერი პირის მიერ (შემდგომში – “ბარათის მფლობელი”) საბანკო ოპერაციის შესრულებას ბანკის მიერ გამოწვებული “ვიზა” ან “მასტერქარდ” პლასტიკური ბარათით (შემდგომში – “ბარათი”) გარდა ბიზნეს-ბარათისა.

* “მობილური ტერმინარი” – უკაბელო გადახდის მონაცემთა.

* “აპლიკაციაში ჩადგმული” – მობილური აპლიკაციის მეშვეობით შესყიდვის განხორციელების შესაძლებლობა იმ გამყიდველებისგან, რომლებიც აპლიკაციაში ანგარიშსწორების მომსახურებას ასრულებენ “სისტემის” მეშვეობით.

* “მხარდაჭერილი მონაცემები” – “მომსახურების გამწევი“-ს “სისტემებთან” თავსებადი მონაცემები.

* “შესამე მხარეებთან გაფორმებული კონტრაქტები” – “მომსახურების გამწევი”, უსაფრთხო კავშირგაბმულობის ოპერატორი, რომლებიც სხვა მხარეებისთვის ითვარისწინებს საკუთარ პირობებს (მათ შორის, “მომსახურების გამწევი

ს პირობებს“) და პერსონალური მონაცემების დაცვის საკუთარ პოლიტიკას.

* “ვირტუალური გამოსახულება” – ციფრული ბარათის ელექტრონული გამოსახულება.

* “თითის ანაბეჭდით შესვლა (Touch ID)” – თითის ანაბეჭდის ამოცნობის ფუნქცია “სისტემაში” მოქმედებების, მათ შორის, ანგარიშსწორების ოპერაციების, დადასტურების მიზნით. ფუნქციის დაყენება, შეცვლა ან გამორთვა შესაძლებელია მობილურ ტერმინალში შესვლის კოდის გამოყენებით.

* უსადენო კავშირგაბმულობის ოპერატორი – ნიშნავს “კლიენტის” მომსახურების გამწევს, რომელიც უზრუნველყოფს მობილურ ქსელთან სატელეფონო კავშირს მობილური ტერმინალის ფუნქციონირებისათვის.

* ანგარიშსწორების მომსახურება –“მომსახურების გამწევი“-ს მომსახურება, რომელიც უზრუნველყოფს საქონელისა და მომსახურებისათვის გადახდას ციფრული ბარათების გამოყენებით და რომელსაც აქვს საკუთარი “პირობები.”

2. ძირითადი დებულებები

2.1. წინამდებარე დოკუმენტი შეიცავს “სისტემაში” “ბანკის” ციფრული ბარათების გამოყენების მარეგულირებელ პირობებს. ეს “პირობები” წარმოადგენს “ბარათის” “კონტრაქტის” დამატებას.

2.2. ამ “პირობებსა” და სხვა “კონტრაქტებს” შორის წინააღმდეგობის არსებობისას, გამოიყენება კონტრაქტის” დებულებები ანგარიშსწორების მომსახურების შესახებ.

2.3. ამ “პირობებით” დადგენილია მხოლოდ “ბანკსა” და “კლიენტს” შორის ურთიერთობებში “კლიენტის” ციფრულ ბარათზე დაშვების და აღნიშნული ბარათის გამოყენების წესები . მობილურ ოპერატორს, “მომსახურების გამწევს” და სხვა, მომსახურე პირებს (მესამე პირებს) ან ანგარიშსწორების მომსახურების სისტემაში შეტანილ ვებ-გვერდებს შეუძლიათ დაადგინონ საკუთარი პირობები და დებულებები (მათ შორის, “მომსახურების გამწევის პირობები”) და პერსონალური მონაცემების დაცვის პოლიტიკა, თუმცა ამავე დროს “კლიენტმა” უნდა დააკმაყოფილოს ასეთ მხარეებთან გაფორმებული კონტრაქტების პირობებიც მათთვის პერსონალური მონაცემების გადაცემისას, მომსახურებით სარგებლობისას ან შესაბამის ვებ-გვერდებზე შესვლისას.

2.4. ციფრული ბარათის მეშვეობით საქონელისა და მომსახურების შესასყიდად “კლიენტის” მიერ ანგარიშსწორების მომსახურებით სარგებლობა რეგულირდება მოქმედი “კონტრაქტით.”

3. მუშაობის პრინციპი

3.1. გადახდის განხორციელება

3.1.1. სისტემით შესაძლებელია “კლიენტის” მობილურ ტერმინალზე “ბარათის” ვირტუალური წარმოდგენის შექმნა, რათა “კლიენტმა” განახორციელოს:

- უკონტრაქტო გადახდები გაყიდვის წერტილებში არსებულ უკონტრაქტო ტერმინალებზე;

- აპრიკაციაში ჩართული ან სხვა ციფრული კომერციული გადახდები იმ გამყიდველების სასარგებლოდ, რომლებიც მიერთებული არიან გადახდების სერვისის სისტემაზე.

3.1.2. კლიენტი “ბარათს” “სისტემაში” არეგისტრირებს “ბარათის” მონაცემების მობილურ ტერმინალში შეყვანით. “ბარათის” წარმატებით ვერიფიკაციის შემთხვევაში, “სისტემა” ქმნის ციფრულ ბარათს და ასევე ქმნის “სისტემაში” მის ვირტუალურ წარმოდგენას.

3.1.3. ციფრული ბარათის საშუალებით ანგარიშსწორების განხორციელების

მიზნით, “კრიენტი” “სისტემაში” ციფრული ბარათის შესაბამისი ვირტუალური წარმოდგენის არჩევისა და გაყიდვის წერტილში მობილური ტერმინალის უკონტაქტო ანგარიშსწორების ტერმინალთან ან წამკითხველთან ახლოს მიტანის შემდეგ ანგარიშსწორებას ადასტურებს აუთენტიფიკაციის მონაცემების შეყვანით.

3.1.4. აპლიკაციაში ჩართული შესყიდვების განხორციელების მიზნით, “კრიენტი” ირჩევს “სისტემაში” ციფრული ბარათის შესაბამის ვირტუალურ წარმოდგენას და ანგარიშსწორებას ადასტურებს აუთენტიფიკაციის მონაცემების შეყვანით.

3.2. ინფორმაციისა და ანგარიშსწორების ნახვა

3.2.1. სისტემა უზრუნველყოფს “კრიენტის” წვდომას ციფრული ბარათის ინფორმაციაზე:

3.2.1.1. ბარათის სტატუსი: მოქმედი, ვადაგასული, დაბლოკილი სხვადასხვა მიზეზის გამო;

3.2.1.2. ინფორმაცია ამ ციფრული ბარათით შესრულებული წინა ოპერაციების შესახებ: თარიღი, შესყიდვის თანხა, გამყიდველის სახელწოდება. “სისტემა” იძლევა თითოეული ციფრული ბარათის შესყიდვის ოპერაციების შესახებ შეტყობინების გამორთვის შესაძლებლობას.

3.2.2. სისტემით შეუძლებელია ინფორმაციის მიღება იმ ოპერაციებზე, რომლებიც “სისტემის” მეშვეობით არ განხორციელებულა.

3.3. კრიენტის უფრებები და მოვარეობები

3.3.1. კრიენტი ვარდებულება დაიცვას “მომსახურების გამწვევის პირობები”

3.3.2. “კრიენტის” “სისტემაში” რეგისტრაციამდე სავარდებულო იმაში დარწმუნება, რომ “კრიენტი” “სისტემაში” რეგისტრირებულია მხოლოდ “კრიენტის” თითის ანაბეჭდებით (Touch ID), სახის ამოცნობით (დაცული აუთენტიფიკაცია) ან “მომსახურების გამწვევის” მიერ მოწოდებული სხვა ახალი ტექნოლოგიით. თითის ანაბეჭდები (Touch ID), სახით იდენტიფიკაცია (დაცული აუთენტიფიკაცია) ან “მომსახურების გამწვევის” მიერ მოწოდებული სხვა ახალი ტექნოლოგია განიხილება “ბარათის” გამოყენებით ოპერაციებზე ტრანზაქციების დადასტურებისას. თუ მობილურ ტერმინალში ავტორიზაციისთვის ან თითის ანაბეჭდის (Touch ID) შესაყვანად ან “კრიენტის” მობილურ ტერმინალზე ოპერაციების შესასრულებლად გამოყენებული იქნება სხვა პირის თითის ანაბეჭდები (ან აუთენტიფიკაციის მონაცემები), ისინი ჩაითვლება “კრიენტის” თითის ანაბეჭდებად (Touch ID).

3.3.3. კრიენტი ვარდებულება აუთენტიფიკაციის მონაცემები შეინახოს მესამე მხარეებისთვის ხერმიუწვდომელ ადგილზე.

3.3.4. აუთენტიფიკაციის მონაცემების ან/და ციფრული ბარათის მონაცემების გატეხვის შემთხვევაში, “კრიენტი” ვარდებულება დაუყოვნებლივ შეატყობინოს “ბანკს” ამის შესახებ.

3.3.5. აუთენტიფიკაციის მონაცემების დაკარგვის ან/და ციფრული ბარათის მონაცემების გატეხვის შესახებ შეტყობინების მიუწოდებლობის ან/და დაგვიანებით მიწოდების შემთხვევაში, “ბანკი” არ არის პასუხისმგებელი “კრიენტის” შესაძლო ზარალზე.

3.3.6. ციფრული ბარათით “კრიენტის” აუთენტიფიკაციის მონაცემების გამოყენებით განხორციელებული ყველა შესყიდვა ან სხვა ოპერაცია განიხილება “კრიენტის” ოპერაციებად.

3.3.7. კრიენტი უფრებამოსიდა გამოიყენოს ციფრული ბარათისთვის ნებისმიერი “ბარათი,” რომელიც აქტიურია “კრიენტის” სახელზე და არ არის დაბლოკილი.

3.3.8. კრიენტი უფრებამოსიდა გამოიყენოს ერთი და იგივე “ბარათი” სხვადასხვა მობილურ ტერმინალში.

3.3.9. კრიენტს აქვს უფრება ნებისმიერ დროს უარი განაცხადოს

“ანგარიშსწორების მომსახურებით” სარგებლობაზე, “სისტემიდან” ციფრული ბარათის წაშლით.

3.4. “ბანკის” უფლებები და მოვადგობები

3.4.1. ბანკი უფლებამოსილია უარი უთხრას “კლიენტს” “ბარათის” რეგისტრაციაზე და “სისტემაში” ციფრული ბარათის შექმნაზე.

3.4.2. ბანკი უფლებამოსილია დაბლოკოს ციფრული ბარათის მოქმედება ან “სისტემაში” მისი გამოყენების შესაძლებლობა, გასცეს ბრძანება “ბარათის”/ციფრული ბარათის ამოღების შესახებ და ამ მიზნით მიიღოს ყველა აუცილებელი ზომა:

3.4.2.1. “კლიენტის” მიერ ამ “პირობებით” გათვარისწინებული ვადლებულებების შეუსრულებლობის ან არასათანადოდ შესრულების შემთხვევაში;

3.4.2.2. ციფრული ბარათის ან/და ბარათის არასანქცირებული გამოყენების შესახებ ეჭვის შემთხვევაში.

3.4.3. “ბანკი” ვადლებულია “კლიენტს” გაუწიოს საინფორმაციო მხარდაჭერა ციფრული ბარათით სარგებლობასთან დაკავშირებით შემდეგ სატელეფონო ნომერზე: + 995 32 2 27 27 27

3.5. მესამე მხარეებთან გაფორმებული კონტრაქტები

3.5.1. ეს “პირობები” მოქმედებს მხოლოდ კლიენტის მიერ ციფრული ბარათ(ებ)ის გამოყენებისას. მომსახურების გამწვევს, უსაღწერო კავშირგაბმულობის ოპერატორს და სისტემაზე მიერთებულ სხვა ვებ-გვერდებს ან მესამე მხარის მომსახურებას აქვთ საკუთარი “კონტრაქტები” მესამე მხარეებთან, და ამავდროულად “კლიენტი” ვადლებულია შეასრულოს მათი პირობები ასეთი პირობისთვის პერსონალური ინფორმაციის მიწოდებისას, მათ მიერ გაწეული მომსახურებით სარგებლობისას ან შესაბამის ვებ-გვერდებზე შესვლისას. ბანკი არ არის პასუხისმგებელი მომსახურების გამწვევის ან მესამე მხარის შინაარსის უსაფრთხოებაზე, სიზუსტეზე, კანონიერებაზე, შესაფერისობაზე ან სხვა ასპექტებზე, პროდუქტებისა თუ მომსახურების ფუნქციონირებაზე.

3.5.2. ბანკი არ არის პასუხისმგებელი და არ უზრუნველყოფს მხარდაჭერას ან დახმარებას მესამე მხარის აპარატული თუ პროგრამული უზრუნველყოფის, აგრეთვე მესამე მხარის პროდუქტებისა თუ მომსახურების (მათ შორის, “სისტემების” ან მობილური ტერმინალის) გამოყენებასთან დაკავშირებით.

3.6. მომსახურების ღირებულება

3.6.1. “ბანკი” არ ითხოვს ანაზღაურებას ციფრული ბარათის გამოყენებისთვის.

3.6.2. კლიენტმა უნდა გაითვარისწინოს ის, რომ მესამე მხარეებთან გაფორმებული კონტრაქტები და ხელშეკრულებები შეიძლება ითვარისწინებდეს ანგარიშსწორების პირობებს, შეზღუდვებს და აკრძალვებს, რომლებმაც შეიძლება გავრენა იქონიოს ციფრული ბარათ(ებ)ის გამოყენებაზე, მაგარიტად, უსაღწერო კავშირგაბმულობის ოპერატორის მიერ მონაცემების გამოყენება ან ტექსტური შეტყობინებების გაგზავნაზე საფასურის დაკისრება. კლიენტი მხოლოდ თავად არის პასუხისმგებელი ამგვარი საფასურის გადახდაზე და ყველა შეზღუდვისა და აკრძალვის დაცვაზე.

3.7. დავების გადაწყვეტა და მარეგულირებელი სამართალი

3.7.1. მხარეთა შორის ნებისმიერი დავა ან უთანხმოება უნდა გადაწყდეს მოლაპარაკების გზით. თუ მხარეები ვერ მიაღწევენ შეთანხმებას, ამგვარი დავა განსახილველად გადაეცემა თბილისის საქარაქო სასამართლოს.

3.7.2 წინამდებარე ხელშეკრულება რეგულირდება საქართველოს კანონმდებლობით.

4. კონფიდენციალურობა და უსაფრთხოება

4.1. პერსონალური ინფორმაცია

4.1.1. კლიენტი გაეცნო და თანახმაა, რომ “ბანკი” უფლებამოსილია

განახორციელოს ტექნიკური, პერსონალური მონაცემებისა და დაკავშირებული ინფორმაციის, მათ შორის და არა მხოლოდ, “კლიენტის” მობილურ ტერმინალზე არსებული ინფორმაციის შეგროვება, დამუშავება და გამოყენება, რათა უზრუნველყოს:

4.1.1.1. “ბანკის” პროდუქტების და მომსახურების გაუმჯობესება კლიენტის სასარგებლოდ;

4.1.1.2. განუვლი მომსახურების უსაფრთხოების გაზრდა.

4.1.1.3. თაღლითობის/ფულის გათეთრების პრევენცია;

4.1.2. დანარჩენ შემთხვევებში, ამგვარი ინფორმაციის გამოყენებაზე და გადაცემაზე ნებართვის გაცემა რეგულირდება ამ “პირობებისა და “პერსონალური მონაცემების დაცვის შესახებ კანონის” შესაბამისად.

4.2. სხვა პირების მიერ შეგროვებული ინფორმაცია

4.2.1. ბანკი არ არის პასუხისმგებელი “სისტემის” მიერ განუვლი მომსახურებაზე ან მესამე მხარის მიერ განუვლი მომსახურებაზე. შესაბამისად, “კლიენტის” მიერ ციფრული ბარათით ან “სისტემით”

სარგებლობისას ,,მომსახურების გამწვევის’’ მიერ შეგროვებული ნებისმიერი ინფორმაცია რეგულირდება ,,მომსახურების გამწვევისა’’ და მესამე მხარეებთან გაფორმებული კონტრაქტებით.

4.3. “კლიენტის” მობილური ტერმინალის დაკარგვა, მოპარვა ან არასანქცირებული გამოყენება:

4.3.1. მობილური ტერმინალის დაკარგვის ან მოპარვის, “ბარათის” (ციფრული ბარათის) ან მისი მონაცემების მესამე მხარის მიერ გამოყენების ან “სისტემის” “კლიენტის” თანხმობის გარეშე გამოყენების შემთხვევაში, “კლიენტი” ვადღებულობს კონკრეტული ფაქტების გამოვლენისთანავე დაუყოვნებლივ შეატყობინოს “ბანკს” აღნიშნულის თაობაზე.

4.3.2. აუთენტიფიკაციის მონაცემების გატეხვის ან გატეხვის ეჭვების შემთხვევაში, “კლიენტი” ვადღებულობს დაუყოვნებლივ შეცვალოს პირადი უსაფრთხოების მონაცემები, აუთენტიფიკაციის მონაცემები და დარწმუნდეს იმაში, რომ მობილურ ტერმინალში არის მხოლოდ გადამწმენილი თითის ანაბეჭდები (Touch ID), რათა თავიდან იყოს აცილებული ციფრული ბარათის ან პირადი ინფორმაციის არასანქცირებული გამოყენება.

4.3.3. ახალი მობილური ტერმინალის მიღებისას, “კლიენტი” ვადღებულობს დარწმუნდეს იმაში, რომ ძველ მობილურ ტერმინალში წაშლილია ყველა ციფრული ბარათი და სხვა პერსონალური ინფორმაცია.

4.3.4. “კლიენტი” ვადღებულობს საჭიროების შემთხვევაში “ბანკს” დაეხმაროს მოკვდევების ჩატარებისას და განახორციელოს თაღლითობის პრევენციის ზომები და სხვა ზომები, რომლებიც შესაძლებელია “ბარათების” უკანონო წვდომის პრევენცია.

4.3.5. “სისტემაში” ან/და მობილურ ტერმინალში შესაძლებელია ციფრული ბარათების არასანქცირებული გამოყენების პრევენციის მიზნით ზოგიერთი ფუნქციისა და უსაფრთხოების ზომის გამოყენება. პასუხისმგებლობა ამგვარ ფუნქციებზე და პროცედურებზე ეკისრება მხოლოდ ,,მომსახურების მიმწოდებელს“. “კლიენტი” ვადღებულობს არ გათიშოს ამგვარი ფუნქციები და გამოიყენოს კონკრეტული ფუნქციები და უსაფრთხოების ზომები ყველა ციფრული ბარათის დაცვის უზრუნველსაყოფად.

4.4. “სისტემის,” სხვა აუთენტიფიკაციის მონაცემების და “ბარათების” (რომლებიც შერჩეულია ციფრული ბარათების სახით გამოსაყენებლად) დაცვა.

4.4.1. “კლიენტი” ვადღებულობს უზრუნველყოს პირადი უსაფრთხოების მონაცემების და აუთენტიფიკაციის მონაცემების კონფიდენციალურობა.

“კლიენტი” ვადღებულობს უზრუნველყოს მათი უსაფრთხოება, აგრეთვე მობილური

ტერმინარის უსაფრთხოება ისევე, როგორც უზრუნველყოფილია ანგარიშსწორების “ბარათების” და კრიენტის ვინაობის დამადასტურებელი სხვა მონაცემების, ნომრების და პაროლების უსაფრთხოება.

4.4.2. ბანკის მკაცრი რეკომენდაციით ციფრული ბარათის უსაფრთხოების შესახებ მონაცემების “კრიენტის” მიერ გამოყენებული მონაცემებისგან ცალკე შენახვა. ანგარიშსწორების ფიზიკური “ბარათები” არ უნდა ინახებოდეს მობილურ ტერმინართან ერთად გარდა “ბარათის” “სისტემაში” რეგისტრაციის შემთხვევებისა.

4.4.3. იმ ოპერაციის შესახებ ტექსტური შეტყობინებების, ან ელ-ფოსტის (რომლითაც “კრიენტი” “სისტემაში” იყო რეგისტრირებული) მიღებისას, რომლის “კრიენტს” არ განუხორციელებია, ან ისეთი ოპერაციების არსებობისას, რომლებიც “კრიენტმა” ვერ იცნო მობილურ ტერმინარზე ან საბარათე ანგარიშის ამონაწერზე, დაუყოვნებლივ მიმართეთ “ბანკს” ტელეფონზე + 995 32 2 2727.

5. ფუნქციის შეჩერება, გაუქმება და შეცვლა

5.1. “ბანკი” იტოვებს უფლებას ნებისმიერი საფუძვლით (შეტყობინების საფუძველზე) შეწყვიტოს ნებისმიერი ციფრული ბარათისა და “სისტემაში” მონაწილეობის მომსახურება ან მხარდაჭერა. “ბანკს” აქვს უფლება დაბლოკოს, შეზღუდოს, შეაჩეროს ან შეწყვიტოს “კრიენტის” მიერ ნებისმიერი ციფრული ბარათის გამოყენება “კრიენტის” მიერ ამ “პირობების,” “კონტრაქტის” და “მომსახურების გამწვევის პირობების,” აგრეთვე მესამე მხარეებთან გაფორმებული კონტრაქტების დარღვევის შემთხვევაში ან თაღლითური საქმიანობის არსებობის ან ციფრული ბარათის ბოროტად გამოყენების შესახებ ეჭვების არსებობისას.

5.2. “მომსახურების გამწვევი” იტოვებს უფლებას დაბლოკოს, შეზღუდოს, შეაჩეროს ან შეწყვიტოს “კრიენტის” მიერ ნებისმიერი ციფრული ბარათის გამოყენება ან/და შეცვალოს “სისტემის” ფუნქცია “ბანკთან” შეთანხმების გარეშე. კრიენტი აცნობიერებს და თანახმაა, რომ ასეთ შემთხვევაში “ბანკი” არ აგებს პასუხს “კრიენტის” ან მესამე მხარის წინაშე.

5.3. თაღლითური მოქმედებების ან საეჭვო საქმიანობის “ბანკის” მიერ გამოვლენის შემთხვევაში, “ბანკს” უფლება აქვს მიიღოს ზომები “ბარათის,” მათ შორის, ციფრული ბარათის დასაბლოკად, რის შესახებაც კრიენტს უნდა ეცნობოს სხვადასხვა ხელმისაწვდომი საშუალებით – ხმოვანი ბარათ, შეტყობინებების გაგზავნის სისტემით [Push Notifications], SMS-ით ან ელ-ფოსტით – შეტყობინების გზით.

5.4. ციფრული ბარათის დროებითი დაბლოკვის ან შეჩერების აღმოფხვრის შემდეგ (მაგ., თაღლითური მოქმედებების არსებობაზე შემოწმების ჩატარების შემდეგ), “კრიენტი” შეძლებს გააგრძელოს “სისტემით” სარგებლობა შესაბამისი შეტყობინების საფუძველზე.

5.5. კრიენტს აქვს უფლება “სისტემაში” წაშალოს ციფრული ბარათი მობილურ ტერმინარზე, არსებულ “სისტემაში” შესაბამისი პროცედურის გავლით ან ამის შესახებ “ბანკისთვის” მიმართვის გზით ტელეფონის ნომერზე + 995 32 2 27 27 27. ასეთ გარემოებებში, კრიენტი “ბანკს” ანიჭებს უფლებას გააგრძელოს ნებისმიერი შეუსრულებელი დავარების დამუშავება ციფრული ბარათის გამოყენებით.

6. შეფერხება ანგარიშსწორების მომსახურების განწვევისას

6.1. ციფრულ ბარათში შესვლა, ციფრული ბარათის გამოყენება და მომსახურება დამოკიდებულია “სისტემისა” და უსაღწერ კავშირგაბმულობის ოპერატორის ქსელის მომსახურების მოცულობაზე. ბანკი არ არის “სისტემის” ან ამგვარი ქსელის მომსახურების ოპერატორი და არ აკონტროლებს მათ საქმიანობას. ბანკი “კრიენტის” წინაშე არ არის პასუხისმგებელი იმ გარემოებებზე, რომლებმაც

შეიძლება შეაფერხოს, დაბრკოლებები შეუქმნას ან სხვაგვარად უარყოფითი გავლენა იქონიოს რომელიმე ციფრული ბარათის ფუნქციონირებაზე, მათ შორის, განაპირობოს “სისტემის” მომსახურების ან უსადენო კავშირგაბმულობის მომსახურების, კომუნიკაციების ხერხიუნჯდომლობა, ქსელის დაგვიანებები, უსადენო დაფარვის შეზღუდვები, სისტემის მწყობრიდან გამოსვლა ან უსადენო კავშირგაბმულობის შეფერხება.

6.2. ციფრული ბარათის გამოყენება ითვალისწინებს პერსონალური ინფორმაციის გადაცემას მესამე მხარის კავშირის მეშვეობით. რადგან “ბანკი” ასეთი კავშირების კონტროლს ან ოპერირებას არ ახორციელებს, ის ვერ იძლევა ამგვარი მონაცემების გადაგზავნის კონფიდენციალურობის ან უსაფრთხოების გარანტიას.

7. პასუხისმგებლობის შეზღუდვა

7.1. “კრიენტი” თანახმაა, რომ “სისტემის” ფუნქციები და ციფრული ბარათი შეიძლება განახდეს ავტომატურად დამატებითი შეტყობინების მიწოდების გარეშე. “ბანკი” იტოვებს უფლებას მიიღოს გადაწყვეტილება ციფრული ბარათის მიერ შესრულებული ოპერაციების სახეების ან/და მოცულობების გაფართოების, შემცირების ან შეჩერების, ან რეგისტრაციის პროცედურაში ცვლილებების შეტანის შესახებ. “სისტემის” ფუნქციებისა და ფუნქციონირების განახლებისა და მოდერნიზაციის უფლება არ მოიცავს “კონტრაქტში” ისეთ ცვლილებას, რომლის შეტანაც მხოლოდ “კონტრაქტის” შესაბამისად არის შესაძლებელი.

8. ცვლილებები “პირობებში”

8.1. “ბანკი” იტოვებს უფლებას ცადმხრივად შეიტანოს “პირობებში” ცვლილებები. “ბანკი” ნებისმიერი ცვლილების შესახებ კრიენტისთვის შეტყობინებას ახორციელებს ელ-ფოსტით ან კომუნიკაციის ნებისმიერი სხვა საშუალების გამოყენებით. კრიენტს აქვს შესაძლებლობა გაეცნოს მობილურ ტერმინალზე შემოთავაზებულ ცვლილებებს. თუ კრიენტი რომელიმე ცვლილებას არ ეთანხმება, ის ვალდებულია ციფრული ბარათი წაშალოს “სისტემიდან” “სისტემაში” “ბარათის წაშლის” ღირავზე დაჭერით.

9. კომუნიკაცია

9.1. მობილურ სისტემაში საბანკო ბარათის რეგისტრაციით “კრიენტი” ავტომატურად ეთანხმება “თიბისი ბანკის” მიერ დადგენილ “პირობებს.”

9.2. კრიენტი აგრეთვე თანახმაა “ბანკის” მიერ გამოგზავნილი შეტყობინებები და სხვა მესიჯები “სისტემის” მომსახურების პირობის შესახებ მიიღოს:

9.2.1. ელ-ფოსტით;

9.2.2. SMS-ით;

9.2.3. შეტყობინებების გაგზავნის სისტემით [Push Notifications];

10. დამატებითი პირობები

10.1. “სისტემაში” გამოყენებისათვის თავსებად მობილურ ტერმინალებთან დაკავშირებით წარმოშობილ ნებისმიერ შეკითხვაზე “კრიენტმა” უნდა მიმართოს უშუალოდ “მომსახურების გამწვეს”.

10.2. “სისტემის” მომსახურების შეზღუდვების ან ღიშტების, აგრეთვე აპლიკაციის პროგრამის მინამაღური მოთხოვნების და აპარატური უზრუნველყოფის შესახებ ინფორმაციის მისაღებად “კრიენტმა” უნდა მიმართოს უშუალოდ “მომსახურების გამწვეს”..

1. Terms and Conditions of use of Bank cards in the mobile payment system

1.1. Terms and Definitions

Each term retains its meaning no matter where it is used in the Terms, and the words for the singular include the plural and vice versa.

* Service Provider – * Any company being the vendor of the Mobile terminal with whom the Client signed the agreement on providing Payment services.

* System – pre-installed software in the Mobile Terminal, exclusive rights to which belong to the Service Provider, and which is an application allowing Mobile terminals to provide Payment Services.

* Service Provider Terms – Software License Agreement and other Additional Service Provider Terms concluded by and between the Client and the Service Provider.

* Bank –TBC Bank Joint-stock company, 0102, #7 Marjanishvili st. Tbilisi, Georgia, ID: 204854595

* Contract – Terms of comprehensive banking services.

* Client – an individual who has entered into an Agreement with the Bank.

* Contactless payment – a payment made by using the Digital Card in a contactless reader.

* Authentication data – the Client's password for authorization in the Mobile Application (including but not limited to biometric data (fingerprint authorization) set in accordance with the Conditions of the Service Provider, PIN code, and other data used to access the System. Authentication data is equivalent to the Client's personal signature.

* Digital Card – A Card that the Client has selected and registered for use in the System.

* Card – Service with a plastic card implies performance of a banking operation through the plastic card "VISA" or "MasterCard" (hereinafter "Card") issued by the bank, except for business card, by the Client (hereinafter "Card Owner") or any person notified by them in a written form (hereinafter "Card Owner").

* Mobile terminal – a wireless payment device.

* Built-in application – the ability to make a purchase using a mobile application from merchants who provide payment services in their applications through the System.

* Supported devices – devices that support the Service Provider Systems.

* Contracts with a third party – the Service Provider, the wireless operator and any other third party services or sites embedded in the System, which provide their own terms and conditions (including the Terms and Conditions of the Service Provider) and privacy policy.

* Virtual representation – an electronic image of a digital card.

* Fingerprint input – fingerprint recognition function to certify actions in the System, including payment transactions. The function can be set, changed or disabled using the access code in the Mobile Terminal.

* Wireless Operator – means the Client's service provider that provides a telephone connection to the mobile network for the operation of the Mobile Terminal.

* Payment Services – Service Provider services for payment for goods and services using Digital Cards in accordance with the Service Provider Terms.

2. General Provisions

2.1. This document contains conditions governing the use of any Digital cards of the Bank in the System. These Terms are an addition to the Card Agreement.

2.2. If there are discrepancies between the provisions of these Terms and other Agreements, the provisions of this Agreement apply to Payment Services.

2.3. These Terms and Conditions establish the rules for access and use of the Client's Digital Card only between the Bank and the Client. The mobile operator, Service Provider and other third-party service providers or sites included in the Payment Services system may set their own terms and conditions (including the terms of the Service Provider) and privacy policy, and the Client must also comply with the terms of such Agreements with third parties when providing them with personal information, using the services or visiting the relevant sites.

2.4. The use of Payment Services by the Client for the purchase of goods and services using a Digital Card is governed by the Agreement in effect.

3. Working principle

3.1. Making payments

3.1.1. The system allows you to create a Virtual Card View on the Client's Mobile Terminal, so that the Client can perform:

- * Contactless payments at contactless terminals at points of sale;
- * Built-in application or other digital commercial payments to sellers connected to the system of Payment services.

3.1.2. The client registers the Card in the System by entering the Card details into the Mobile terminal. After successful verification of the Card, the System forms a Digital Card and creates its Virtual Representation in the System.

3.1.3. To make a payment with the Digital Card, the Client, by selecting the appropriate Virtual Representation of the Digital Card in the System and placing the Mobile Terminal next to the contactless payment terminal at the point of sale or a reader, the Client confirms the payment by entering Authentication data.

3.1.4. To make purchases with the Embedded application, the Client selects the appropriate Virtual Representation of the Digital Card in the System and confirms the payment by entering Authentication data.

3.2. Browsing the information and the payments

3.2.1. The system provides the Client with an access to the following information on the Digital Card:

3.2.1.1. card status: active, expired, blocked due to different reasons;

3.2.1.2. information on previous transactions performed by this Digital Card: date, amount of purchase, name of the seller. The System provides the ability to disable notification of purchase transactions for each Digital Card.

3.2.2. The system cannot provide information on transactions performed without using the System.

3.3. Rights and obligations of the Client

3.3.1. The Client is obliged to comply with the terms of the Service Provider.

3.3.2. Before registering in the System, the Client is obliged to ensure that only the Client's fingerprints (Touch ID), Face ID (secure authentication) or other new technology provided by the Service Provider are registered in the System. Usage of fingerprints (Touch ID), Face ID (secure authentication) or other new technology provided by the Service Provider will be considered as the confirmation of transactions on operations with the use of the Card. If fingerprints (or Authentication Data) of another person are used for the authorization in the Mobile terminal or for the Fingerprint Login (Touch ID), or for performing operations at the Client's Mobile Terminal, such fingerprints will be considered as the Client's fingerprints.

3.3.3. The client is obliged to ensure the storage of their Authentication data in a place inaccessible to third parties.

3.3.4. In the event of a compromise of the Authentication data and / or Digital Card data, the Client must immediately notify the Bank about such case.

3.3.5. In case the Client fails to timely notify the Bank by about the loss of the Authentication data and / or the compromise of the Digital Card details, the Bank shall not be liable for any losses of the Client.

3.3.6. Purchases or other transactions made by the Digital Card and Client Authentication data are considered Client operations.

3.3.7. The Client has the right to use any Card opened in the name of the Client that is not canceled or blocked, to create a Digital Card.

3.3.8. The Client has the right use one and the same Card in different Mobile terminals.

3.3.9. The Client has the right to refuse to use the Payment Services at any time by deleting the Digital Card from the System.

3.4. Rights and Obligations of the Bank

3.4.1. The Bank is authorized to refuse the Client to register the Card and create a Digital Card in the System.

3.4.2. The Bank is authorized to block the operation of the Digital Card or the possibility of its use in the System, to order a removal of the Card / Digital Card and take all necessary measures for this:

3.4.2.1. in case of non-fulfillment or improper fulfillment by the Client of the obligations stipulated by these Terms;

3.4.2.2. in case an unauthorized use of a Digital Card and / or Card is suspected.

3.4.3. The Bank is obliged to provide information support to the Client on the use of the Digital Card by phone: +995 32 2 27 27 27.

3.5. Agreements with third parties

3.5.1. These Terms apply only to the use of the Digital Card(s) by the Client. The service provider, wireless operator and other third-

party sites or services connected to the System have their own Agreements with third parties, and the Client is obliged to comply with their conditions when providing personal information to specified persons, using the services provided by them or visiting relevant sites. The Bank is not responsible for the safety, accuracy, legality, suitability and other aspects of the content or operation of the products or services of the Service Provider or of a third party.

3.5.2. The Bank is not responsible and does not provide support or assistance in relation to any third party hardware or software, as well as their other products or services (including the System or the Mobile Terminal).

3.6. Service price

3.6.1. The bank does not charge for the use of the Digital Card.

3.6.2. The Client must consider that contracts and other agreements with third parties may include payments, restrictions and prohibitions that may affect the use of any Digital Card(s), for example, data usage or text messaging fees charged by the wireless operator. The client undertakes an obligation to bear sole responsibility for such payments and the observance of all restrictions or prohibitions.

3.7. Resolution of Disputes and the governing law

3.7.1. Any dispute and disagreement between the parties are to be resolved by negotiations. In case an agreement between the parties is not reached, such dispute shall be transferred to the Tbilisi City Court.

3.7.2. 3.7.2 This agreement is governed by Georgian law.

4. Privacy and security

4.1. Personal Information

4.1.1. The Client has read and agrees that the Bank is entitled to collect, process and use technical, personal data and related information, including but not limited to, the Client's Mobile Terminal, in order to ensure:

4.1.1.1. Improvement of the Bank's products and services for the benefit of the client;

4.1.1.2. improving safety of the services provided;

4.1.1.3. prevention of fraud and money laundering;

4.1.2. In the remaining cases, permission to use and transfer such information is governed by these Terms, the Law on personal data protection.

4.2. Information collected by other persons

4.2.1. The Bank is not responsible for the services of the System or another third-party Service Provider. Accordingly, any information, collected by the Service Provider when a Client uses a Digital Card or System, is governed by the contracts with the Service Provider and Third Parties.

4.3. Loss, theft or unauthorized use of the Client's Mobile Terminal

4.3.1. In case of loss or theft of the Mobile Terminal, use of the Card (Digital Card) or its details by a third party or use of the System without the Client's consent, the Client is obliged to notify the Bank immediately after the discovery of such facts.

4.3.2. In the event of a compromise or suspicion of compromising the Authentication data, the Client is obliged to immediately change the personal security information, Authentication data and make sure that only authorized fingerprints (Touch ID) are registered in the Mobile terminal in order to avoid any unauthorized use of the Digital card or personal information.

4.3.3. Upon receipt of the new Mobile Terminal, the Client is obliged to ensure that all Digital Cards, other personal information in the replaced mobile terminal are erased.

4.3.4. If needed, the client is obliged to assist the Bank in conducting any investigations and take measures to prevent fraud or other measures that may prevent unauthorized access to the Cards.

4.3.5. Certain functions and security measures may be used in the System and / or in the Mobile Terminal to ensure protection from unauthorized use of Digital Cards. Responsibility for such functions and procedures rests solely with the Service Provider. The Client undertakes not to disable such functions and use the specified functions and security measures to ensure the protection of all Digital Cards.

4.4. Protection of system, other authentication data and the Cards (which are selected to be used as digital cards).

4.4.1. The client is required to ensure the confidentiality of personal security information and authentication information. The Client is obliged to ensure their safety, as well as the safety of the Mobile Terminal in the same way that the safety of Bank Cards and other information, numbers and passwords confirming the Client's identity are ensured.

4.4.2. The Bank strongly recommends that the security information of the Digital Card be kept separately from the information used by the Client. Physical Bank Cards should not be stored with a Mobile Terminal, except for cases of Card registration in the System.

4.4.3. When you receive a text message, an e-mail stating that the Client has registered with the System, provided that the Client has not performed such registration, or if there are any operations that the Client did not recognize on the Mobile terminal or in the Card statement, immediately contact the Bank by phone: + 995 32 2 2727.

5. Pausing, changing and cancellation of the functions

5.1. The Bank reserves the right to terminate the service or support of any Digital Card or participation in the System for any reason (on the basis of a notice). The Bank has the right to block, restrict, suspend or terminate the use of any Digital card by the Client in case of violation of these Terms, the Agreement, the Service Provider Terms and Conditions, as well as agreements with third parties, or if the Bank suspects fraudulent activity or abuse of the Digital Card.

5.2. The Service Provider reserves the right to block, restrict, suspend or terminate the use of the Digital Card by the Client and / or change the System functions without the consent of the Bank. The Client understands and agrees that in this case the Bank shall not be liable to the Client or a third party.

5.3. If the Bank detects fraud or any suspicious activity, the Bank has the right to take measures to block the Card, including the Digital Card, by notifying the client in different available ways: by a voice call, Push notification, SMS message or email.

5.4. After the temporary blocking or suspension of the Digital Card has been eliminated (for example, after carrying out a revision for fraud), the Client will be able to continue using the System services based on a corresponding notification.

5.5. The Client has the right to remove the Digital Card from the System by following the corresponding procedure in the System on the Mobile Terminal or contact the Bank by phone: 995 32 2 27 27 27 . In such circumstances, the client authorizes the Bank to continue processing of any non-fulfilled orders using the Digital Card.

6. Interruptions in the provision of Payment Services

6.1. Access, use and maintenance of a Digital Card depends on the scope of services of the System and the network of the wireless operator. The Bank is not the operator of the System or such network services and does not control their actions. The Bank shall not be liable to the Client for any circumstances that may interrupt, create obstacles or otherwise affect the operation of any Digital Card, including unavailability of the System or wireless services, communications, network delays, wireless coverage restrictions, system interruptions or interruption of wireless communications.

6.2. The use of a Digital Card envisages electronic transfer of personal information through a third party connection. Since the Bank does not operate or control such connections, the Bank cannot guarantee the confidentiality or security of such data transmission.

7. Disclaimer

7.1. The Client agrees that the functions of the System and the Digital Card may be updated automatically without any additional notice. At any time, the Bank may decide to expand, reduce or suspend the types and / or volumes of operations provided by the Digital Card, or change the registration procedure. The right to update and modify the functions and functionality of the System does not include changes to the Agreement, which can be made only in accordance with the Agreement.

8. Changes to these Terms

8.1. The Bank reserves the right to unilaterally revise these Terms and Conditions in accordance with the Agreement. Any changes to these Terms and Conditions shall be communicated by the Bank to the Client via e-mail or using any other method of communication. The client has the opportunity to get acquainted with the revised Terms and Conditions on the mobile terminal. If the Client does not accept any changes made to these Terms, he is obliged to delete their Digital Card from the System by clicking on the "Delete Card" button in the System.

9. Communication

9.1. By registering the Card in the System, the Client automatically accepts Terms and Conditions stipulated by the TBC Bank.

9.2. The Client also agrees to receive notifications and other

messages sent by the Bank regarding the status of the System services in the following ways:

9.2.1. Email

9.2.2. SMS messages;

9.2.3. Push Notifications;

10. Additional provisions

10.1. For any questions related to the support of Mobile terminals compatible with the System, the Client must contact the Service Provider directly.

10.2. For information about any restrictions or limits in relation to the System services, as well as minimum software and hardware requirements, the Client is obliged to contact the Service Provider directly.

Touch ID and Face ID are trademarks of Apple Inc., registered in the U.S. and other countries.