

APROBAT  
la ședința Comitetului de Conducere  
al BC „EuroCreditBank” S.A.  
proces-verbal nr.104  
din 12.06.2023

Termeni și condiții de atașare  
a cardurilor emise de  
BC" EuroCreditBank" S.A.  
în portofele electronice

## CAPITOLUL 1. Noțiuni generale

### 1. Prevederi generale

1.1. Prezenții Termeni și condiții de atașare a cardurilor emise de BC "Eurocreditbank" S.A. în portofele electronice (în continuare Termeni și condiții), stabilite de BC "Eurocreditbank" S.A. (în continuare Bancă), descriu modul de atașare și utilizare a cardurilor de plată eligibile în :Apple Pay.

Pe tot parcursul textului se utilizează mărcile comerciale ale Apple Inc. înregistrate în SUA, în alte țări și regiuni: Apple Pay, Apple, Apple Wallet, Apple Watch, Face ID, Find My, iPad, iPhone, App Store, iCloud.

1.2. Prezenții Termeni și condiții completează și detaliază relația contractuală existentă între deținătorul cardului și Bancă, stabilite în baza Condițiilor Generale Bancare, Cererea de deschidere a contului și emitere a cardului și Tarifele și limitele privind deservirea cardurilor bancare emise de BC "Eurocreditbank" S.A.

Condițiile Generale Bancare și Tarifele și limitele privind deservirea cardurilor bancare emise de

BC "Eurocreditbank" S.A. sunt accesibile pe panoul informativ în cadrul subdiviziunilor Băncii și pe pagina web a Băncii.

1.3. Prezenții Termeni și condiții guvernează atașarea, activarea și utilizarea cardurilor eligibile emise de Bancă în Apple Pay.

1.4. Banca permite utilizarea cardurilor eligibile emise de Bancă în aplicațiile Apple Pay în vederea efectuării operațiunilor de plată.

1.5. Prezenții Termeni și condiții reglementează accesul și utilizarea cardului în aplicațiile Apple Pay numai între client, în calitate de deținător de card și Bancă.

1.6. Furnizorii de dispozitive prin intermediul cărora se pot efectua plăți prin intermediul aplicațiilor Apple Pay sau terți cu care aceștia colaborează pot avea proprii termeni și condiții.

1.7. Prezenții Termeni și condiții nu se aplică pentru serviciile/produsele achiziționate de la furnizorul dispozitivului, al rețelei de telefonie mobilă și nici de pe alte pagini, sau servicii care aparțin terților care integrează sau permit furnizarea Apple Pay. Banca nu răspunde pentru legalitatea furnizării / prestării produselor / serviciilor furnizorului dispozitivului și / sau ale terților, nici pentru securitatea, precizia, legalitatea sau orice alt aspect al respectivelor produse / servicii oferite de aceștia.

1.8. Pentru informații suplimentare despre Apple Pay, deținătorul cardului poate accesa compartimentul Apple Wallet și/sau Apple Pay pe pagina [www.apple.com](http://www.apple.com).

## CAPITOLUL 2. TERMENI ȘI DEFINIȚII

### 2. Noțiuni utilizate

În cuprinsul prezentului document termenii de mai jos vor fi înțeleși după cum urmează:

- Apple – Apple Distribution International cu sediul în Hollyhill Industrial Estate, Cork, Irlanda

furnizor al Apple Pay.

- Aplicație Apple Pay – o platformă de plată oferită de Apple Distribution International, prin

intermediul căreia utilizatorul poate atașa cardurile eligibile pentru a efectua plăți la comercianți,

plăți pe internet, retrace numerar la ATM-urile contactless prin intermediul dispozitivelor Apple.

- Card eligibil pentru atașare și utilizare în Apple Pay – card de plată activ a sistemului internațional Visa Inc., de debit și/sau credit, emis de Bancă pe numele deținătorului de card, în conformitate cu contractul încheiat între deținător și Bancă.

- CVV2 – un cod de securitate din 3 cifre tipărit pe partea verso a cardului.

- Deținător de card – persoana fizică pe numele căreia este emis un card de debit și/sau credit

principal, secundar sau card corporativ, după caz.

- Dispozitiv compatibil Apple Pay – smartfone, tabletă, smartwatch sau alt tip de dispozitiv care

permite efectuarea de plăți prin Apple Pay. Aceste dispozitive sunt prezentate pe pagina [www.apple.com](http://www.apple.com).

- Find My iPhone – o aplicație utilizată pentru localizarea și protecția dispozitivelor de tipul: iPhone, iPad, Apple Watch etc. în cazul pierderii sau furtului.

- Face ID – recunoaștere facială a deținătorului de card, posesor al dispozitivului și se bazează pe autentificare securizată ce permite identificarea geometriei feței.

- FingerPrint – recunoașterea amprentei digitale a deținătorului de card posesor al dispozitivului.

- iCloud – serviciul ce permite stocarea conținutului dispozitivelor Apple.

- Parola de unică folosință (OTP) – parola generată și transmisă de către Bancă în adresa

deținătorului (prin intermediul operatorului de telefonie mobilă cu care Banca a încheiat contract) în cadrul unui mesaj SMS la numărul de telefon al deținătorului de card înregistrat în sistemele informaționale ale Băncii.

- Portofel electronic – Apple Pay.

- Verificarea deținătorului cardului – procedura de autentificare a deținătorului cardului. La atașarea cardului eligibil în portofel electronic, verificarea deținătorului se efectuează prin introducerea parolei de unică folosință de către deținătorul cardului. Durata parolei de unică folosință este limitată și este determinată de Bancă (30 minute). Condițiile, cazurile și frecvența cu care se solicită introducerea parolei pentru verificarea deținătorului la efectuarea tranzacțiilor sunt stabilite de furnizori.

- Token – o serie unică de cifre în format digital ce asigură substituirea securizată a PAN-ului cardului.
- Tokenizare – un proces de înlocuire a unui element de date confidențiale (PAN) cu un echivalent neconfidențial, numit token, care nu are semnificație/valoare independentă pentru uz extern sau intern și este utilizat în domeniul securității informațiilor.
- Near Field Communication (NFC) – un standard utilizat în cazul dispozitivelor electronice prin intermediul căruia se stabilește o comunicație de radio de înaltă frecvență ce permite schimbul wireless de date pe o distanță foarte scurtă, de până la 10 centimetri fiecare.

### CAPITOLUL 3. Descrierea generală Apple Pay

3.1. Banca oferă deținătorilor de card posibilitatea de atașare a cardului în Apple Pay prin acceptarea prezențelor Termenilor și condițiilor.

3.2. Pentru a utiliza cardul în Apple Pay, deținătorul cardului trebuie să dispună de dispozitiv compatibil Apple Pay.

3.3. Funcționalitatea de bază Apple Pay constă în efectuarea tranzacțiilor prin tehnologia contactless prin intermediul cardului de plată, tokenizat în Apple Pay

3.4. Apple Pay permite atașarea unui număr de până la 10 (zece) carduri de plată.

3.5. Banca oferă posibilitatea de a adăuga un singur card pe maximum 10 dispozitive Apple Pay concomitent. Furnizorul de dispozitive poate impune limitări sau restricții și / sau poate avea cerințe minime de software și hardware pentru dispozitivul compatibil utilizat.

3.6. Pentru atașarea și utilizarea cardurilor în Apple Pay, deținătorul de card trebuie să îndeplinească următoarele condiții:

3.6.1. să dispună de dispozitiv Apple, așa cum acestea sunt indicate pe pagina Apple:

[www.apple.com](http://www.apple.com) .

3.6.2. dispozitivul Apple pe care se dorește atașarea cardului să conțină tehnologia NFC activă și sistemul de operare indicat de Apple.

3.6.3. să aibă înregistrat în sistemele Băncii un număr de telefon mobil care aparține unuia din operatorii din RM.

3.6.4. să dețină cel puțin un card eligibil.

3.6.5. să îndeplinească condițiile pentru înregistrare ca utilizator în Apple Pay și orice alte cerințe stabilite și/sau solicitate de Apple pentru utilizarea aplicației, menționate pe pagina Apple. Banca nu are nici o responsabilitate față de deținătorul de card referitor la cerințele/condițiile și/sau orice limitări/restricții privind utilizarea

aplicației stabilite de către Apple și nici la modificarea și/sau comunicarea acestora deținătorului de card.

3.7. Banca nu percepe comision sau altă plată pentru utilizarea cardurilor în Apple Pay. Furnizorul dispozitivului Apple Pay și / sau terții pot percepe taxe, pot impune limitări și restricții care ar putea afecta utilizarea oricărui card emis de Bancă în Apple Pay. Clientul este responsabil pentru plata acestor taxe și se obligă să respecte orice limitări sau restricții impuse.

#### Capitolul 4. Atașarea cardului eligibil în Apple Pay

4.1. Pentru atașarea cardului în Apple Pay, deținătorul de card trebuie să îndeplinească cel puțin condițiile specifice pentru înregistrare ca utilizator al dispozitivului:

- să dețină un dispozitiv compatibil.
  - să dețină un cont de tipul Apple ID pentru serviciile oferite de Apple, autentificat în cadrul serviciului iCloud .
  - să seteze una din modalitățile de blocare/deblocare a ecranului pe dispozitivul (parola, fingerprint, Face ID).

4.2. Cerințele menționate în pct. 4.1 sunt condiții impuse de furnizorul aplicației, Banca nu are nici o responsabilitate în legătură cu cerințele stabilite.

4.3. După îndeplinirea condițiilor de mai sus, deținătorul:

- va accesa în aplicația Apple aplicația Wallet de pe dispozitivul Apple, aplicație care este supusă termenilor și condițiilor Apple.

- va iniția introducerea datelor aferente cardului: va scana sau introduce manual în Apple Pay datele: numele și prenumele, numărul cardului, data de expirare, și va introduce codul CVV2.

- va accepta prezentele Termeni și condiții care vor fi afișate în Apple Pay.

- va introduce în aplicație codul de verificare (OTP) pentru autentificarea deținătorului ca posesor al cardului. În cazul în care solicitarea de atașare este respinsă, deținătorul poate contacta Serviciul suport carduri pentru a obține informație cu privire la această situație.

#### CAPITOLUL 5. Utilizarea cardului/token-ului prin Apple Pay

5.1. Atașarea cardului în Apple Pay generează token al cardului pentru efectuarea plăților prin Apple Pay. Numărul tokenului este diferit de numărul cardului atașat în Apple Pay, acest fapt duce la creșterea securității tranzacțiilor.

5.2. Pentru fiecare atașare a aceluiași card pe dispozitive Apple diferite, se va genera un token diferit asociat dispozitivului respectiv.

5.3. Tokenul generat în Apple Pay poate fi utilizat pentru:

- Plăți contactless la comercianți – prin apropierea dispozitivului de terminalul de plată al comerciantului (ex.POS). Această acțiune se efectuează prin deblocarea dispozitivului mobil prin

- Fingerprint / Face ID / introducerea parolei, în cazul Apple Watch – prin dublu click efectuat pe

- butonul lateral al dispozitivului.

- Plăți pe pagini care afișează opțiunea „buy with Apple Pay” prin tastarea butonului la achitarea comenzii. Această acțiune se efectuează prin deblocarea dispozitivului mobil prin Fingerprint / Face ID / introducerea parolei, în cazul Apple Watch – prin dublu click efectuat

- pe butonul lateral al dispozitivului.

- Retrageri de numerar la ATM-urile contactless. Pentru retragere de numerar va fi necesar și

- introducerea PIN-ului cardului pe terminalul ATM la care se efectuează retragerea. Această acțiune se efectuează prin deblocarea dispozitivului mobil prin Fingerprint / Face ID / introducerea parolei, în cazul Apple Watch – prin dublu click efectuat pe butonul lateral al dispozitivului.

5.4. În cazul în care deținătorul de card și-a atașat mai multe carduri eligibile în Apple Pay, atunci primul card atașat pe dispozitiv va fi selectat implicit la efectuarea plăților. Utilizatorul de card are posibilitatea să modifice oricând cardul selectat ca implicit pentru plăți în Apple Pay.

5.5. În cadrul aplicației Apple Pay, furnizorul va pune la dispoziția deținătorului de card informații referitoare la ultimele 10 tranzacții efectuate cu tokenul asociat dispozitivului.

5.6. La expirarea termenului de valabilitate indicat pe partea din față a Cardului înregistrat în Apple Pay, Tokenul aferent va putea fi utilizat doar în urma înregistrării în Apple Pay a Cardului reinnoit.

5.7. La reemiterea cardului tokenul aferent nu va putea fi utilizat în continuare în Apple Pay. Tokenul aferent va putea fi utilizat doar în urma înregistrării în Apple Pay a Cardului nou.

5.8. Dacă cardul de plată este blocat de către client, plățile prin Apple Pay vor fi disponibile.

Dacă cardul de plată va fi blocat de către Bancă sau la contul de card vor fi aplicate măsuri de interdicție (suspendare, sechestrare în limita sumei blocate etc.) plățile prin Apple Pay nu vor fi disponibile.

5.9. Toate limitele/condițiile stabilite pentru un card de plată conform Condițiilor Generale Bancare și Tarifelor și limitelor privind deservirea cardurilor bancare emise de BC "Eurocreditbank" S.A. sunt valabile și pentru cardul atașat în Apple Pay.

## CAPITOLUL 6. Administrarea tokenului (blocarea/deblocarea) în Apple Pay

6.1. Tokenul poate fi blocat/deblocat prin intermediul Serviciului suport carduri.

6.2. Tokenul blocat poate fi deblocat de către Serviciul suport carduri în dependență de statutul blocării tokenului și doar în cazul în care clientul a fost identificat.

6.3. Clientul are posibilitatea de a șterge cardul din aplicația Apple Pay din dispozitivele Apple Pay folosind aplicația Find My Phone, iCloud.com sau direct din portofel electronic.

Notă: Pentru informații suplimentare despre modalitățile de ștergere a cardului din aplicațiile de pe dispozitivele Apple deținătorul cardului poate accesa pagina [www.apple.com](http://www.apple.com). Clientul poate suspenda dispozitivul Apple Pay prin plasarea acestuia în modul pierdut folosind aplicația din setările telefonului - Find My Phone.

## CAPITOLUL 7. Încetarea utilizării cardurilor prin Apple Pay

7.1. Încetarea de utilizare a cardului fizic de către deținătorul de card, nu încetează în mod automat posibilitatea utilizării acestuia pentru tranzacțiile prin Apple Pay.

7.2. Deținătorul de card poate renunța la utilizarea aplicației, prin eliminarea cardului atașat din aplicația Apple Pay în orice moment. Acest fapt nu va influența posibilitatea utilizării cardului fizic.

7.3. În situație în care furnizorul de dispozitive și/sau al aplicației Apple Pay suspendă, blochează, întrerupe utilizarea aplicației Apple Pay și/sau modifică funcționalitatea acesteia în mod corespunzător se va întrerupe sau modifica posibilitatea de utilizare a cardurilor în aplicația Apple Pay.

## CAPITOLUL 8. Securitatea Apple Pay

8.1. Deținătorul de card este obligat să asigure confidențialitatea informației înregistrate în portofelele electronice, să întreprindă măsuri de protejare și să nu admită utilizarea acesteia de către terțe persoane.

8.2. Deținătorul de card este responsabil pentru utilizarea și tranzacțiile efectuate cu cardul în portofelele electronice, inclusiv și de către terți cărora deținătorul de card le-a oferit acces voluntar sau involuntar la card/dispozitiv, sau la alte detalii de securitate.

8.3. Pentru a preveni accesul neautorizat, Banca recomandă următoarele:

- păstrarea continuă a dispozitivului în siguranță și în posesia deținătorului;
- păstrarea informațiilor de securitate și a parolelor de acces în maximă siguranță și necomunicarea acestora altor persoane;

- setarea parolelor de securitate în corespundere cu cerințele securității informaționale;

- păstrarea cardurilor în format fizic și /sau a detaliilor cardurilor separat de dispozitivul utilizat ș.a.

8.4. Apple Pay poate utiliza anumite funcționalități și proceduri de Securitate pentru a proteja împotriva utilizării neautorizate a oricărui card. Aceste funcționalități și proceduri aparțin exclusiv furnizorului de dispozitive.

8.5. Înainte de a introduce datele cardului în portofelul electronic, deținătorului de card i se va solicita setarea parolei/detaliilor de securitate, pe care le va utiliza pentru accesarea acestora. Condițiile, cazurile și frecvența cu care se solicită introducerea acestei parole / detaliilor de securitate sunt stabilite de furnizorii portofelelor electronice.

8.6. Banca nu poartă răspundere pentru tranzacțiile efectuate cu cardul emis de Bancă și atașat în portofelele electronice până când nu îi este adus la cunoștință producerea unui eveniment sau pînă când nu se solicită blocarea tokenului.

8.7. Apple Pay pot utiliza anumite funcționalități și proceduri de securitate pentru a se proteja împotriva utilizării neautorizate a oricărui card. Aceste funcționalități și proceduri aparțin exclusiv furnizorului de dispozitive. Prin atașarea cardului emis de Bancă în portofelele electronice, deținătorul de card este de acord să nu dezactiveze niciuna dintre caracteristici de securitate și să le utilizeze pentru a proteja toate cardurile emise de Bancă și înregistrate în aplicații. Banca nu controlează aceste metode de securitate și nu răspunde pentru modul în care Apple și / sau furnizorul de dispozitiv compatibil le utilizează.

8.8. În cazul în care deținătorul de card a depistat că dispozitivul mobil, dispozitivul Apple, cardul și/sau alte date au fost compromise este necesar de a elimina cardul conectat la Apple Pay.

## CAPITOLUL 9. Responsabilitățile părților

9.1. Banca oferă informații despre tranzacțiile realizate cu cardurile emise de Bancă și atașate în portofelele electronice în modalități agreeate de Bancă (ex. extras de cont, WEB Banking, etc).

Tranzacțiile efectuate vor fi afișate fără a se indica faptul că au fost efectuate prin intermediul serviciului Apple Pay.

9.2. Banca este în drept să blocheze, să restricționeze, să suspende sau să înceteze oferirea posibilității de utilizare a oricărui card emis de Bancă în Apple Pay dacă se încalcă prezenții Termeni și condiții sau dacă se suspectează orice activitate frauduloasă sau necorespunzătoare a cardului în aplicații.

9.3. Banca nu poartă răspundere dacă furnizorul de dispozitive impune limitări sau restricții pentru utilizarea Apple Pay și/sau poate avea cerințe minime de software și hardware pentru dispozitivul compatibil utilizat.



9.4. Banca nu poartă răspundere față de deținătorii de card ai Băncii care și-au atașat cardul în Apple Pay, în cazul în care furnizorul de dispozitive și/sau al Apple Pay își blochează, restrânge, suspendă sau întrerupe utilizarea Apple Pay.

9.5. Banca nu poartă răspundere și nu oferă suport sau asistență pentru niciun fel de hardware, software sau alte produse sau servicii ale terților. În cazul apariției cărorva întrebări sau probleme cu un produs sau serviciul oferit de Apple sau de un terț, este necesar de a contacta respectivul furnizor / terț pentru asistență.

9.6. Banca nu poartă răspundere pentru accesul, utilizarea token-ului creat în Apple Pay, acestea depind de Apple Pay și de rețeaua furnizorului de internet.

Banca nu operează cu Apple Pay sau astfel de rețele și nu are control asupra operațiunilor lor. Banca nu va răspunde pentru nici o situație care întrerupe, împiedică sau afectează în alt fel funcționarea oricărui card emis de Bancă în Apple Pay precum, dar fără a se limita la indisponibilitatea serviciului Apple Pay sau a serviciului de internet, comunicații, întârzieri în rețea, limitări privind acoperirea rețelei de internet, întreruperi ale sistemului.

9.7. Banca nu este responsabilă pentru pierderile, daunele morale sau patrimoniale cauzate de nerespectarea de către client a prezențelor Termeni și condiții.

9.8. Banca nu este responsabilă pentru prejudiciile rezultate din executarea unor plăți neautorizate generate de expunerea dispozitivului deținătorului de card la viruși și/sau alte aplicații/programe, precum și de furtul acestuia.

9.9. Deținătorul de card poartă răspundere pentru:

- Confidențialitatea parolelor de unică folosință, parolelor, codului PIN și al altor mijloace de acces la dispozitivul mobil, aplicația mobilă, cardul, token-ul;
- Limitarea de acces la dispozitivul mobil / dispozitiv Apple, existența și actualizarea programelor antivirus instalate pe dispozitivul mobil;
- Nepermiterea utilizării de către persoanele terțe a dispozitivului mobil pe care a fost instalată aplicația mobilă;
- Operațiunile efectuate cu ajutorul serviciului Apple Pay pe dispozitivul deținătorului;
- Informarea imediată a Băncii referitor la necesitatea blocării cardului/token-ului sau ștergerea cardului/tokenului;
- Eliminarea cardului din aplicația mobilă înainte de a elimina aplicația mobilă din dispozitivul mobil;
- Eliminarea cardului înainte de distrugerea dispozitivului mobil și înainte de transmiterea dispozitivului mobil în utilizare / în proprietate unei persoane terțe;
- Executarea instrucțiunilor și regulilor de lucru cu aplicația mobilă.

9.10. Deținătorul de card are obligația de:

- a lua măsuri de siguranță, de a consulta și de a respecta condițiile de securitate impuse de Apple, cât și de a efectua toate indicațiile Apple pentru a evita utilizarea neautorizată a token-ului.

- a-și atașa cardul în aplicația Apple Pay doar pe dispozitivele care le deține în mod legal, precum și de a lua măsuri de siguranță pentru a evita utilizarea neautorizată a token-ului.

- a anunța Banca atunci când cardul atașat și/sau dispozitivul pe care a fost atașat cardul a fost pierdut/furat ori folosit fără acordul său și de a bloca token-ul asociat acestuia conform cap.7. În caz contrar, Banca nu va fi responsabilă pentru plățile efectuate cu token în cazul apariției unor evenimente enumerate anterior.

- a păstra în siguranță datele sale de autentificare în Apple Pay și/sau pentru contul său Apple ID și/sau pentru dispozitivul său. Banca nu este responsabilă pentru plățile cu token dacă aceste plăți sunt efectuate de către alte persoane.

- a monitoriza tranzacțiile efectuate cu token și în caz de careva nereguli să comunice imediat Băncii prin apelarea la Serviciul suport carduri.

## CAPITOLUL 10. Dispoziții finale

10.1. Banca va informa deținătorii de card privind modificarea prezențelor Termeni și condiții de utilizare prin afișarea versiunii(lor) modificate a(ale) acestui document pe pagina Web a Băncii ([www.ecb.md](http://www.ecb.md)) și panoul informațional în cadrul subdiviziunilor Băncii.

10.2. Dacă există o neconcordanță între termenii Apple Pay Connect și prezenții Termeni și condiții, se vor aplica prezenții Termeni și condiții pentru tranzacțiile efectuate cu cardul emis de Bancă în Apple Pay.

10.3. Deținătorul de card poate contacta Banca prin intermediul Serviciului suport carduri la numărul de telefon +373 22 50-02-20 pentru orice problemă legată de atașarea, blocarea/deblocarea, ștergerea unui card sau executarea plăților efectuate cu carduri în portofele electronice.

10.4. Prezentul document intră în vigoare la data de 12.06.2023.

APPROVED

at the meeting of the Management Committee  
of BC "EuroCreditBank" S.A.

Minutes No. 104

dated June 12, 2023

Terms and Conditions

for attaching to electronic wallets

the cards issued by BC "EuroCreditBank" S.A.

## CHAPTER 1. General notions

### 1. General provisions

1.1. Present Terms and conditions for attaching in the electronic wallets cards issued by BC "Eurocreditbank" S.A (hereinafter Terms and Conditions), established by BC "Eurocreditbank" S.A. (hereinafter Bank), describe how to attach and use eligible payment cards in Apple Pay.

Throughout the text are used the following trademarks of Apple Inc. registered in the USA and other countries and regions : Apple Pay, Apple, Apple Wallet, Apple Watch, Face ID, Find My, iPad, iPhone, App Store, iCloud.

1.2. The present Terms and Conditions completes and details the existing contractual relationship between the card holder and the Bank, established on the basis of the General Banking Conditions, the Application for opening the account and issuing the card and the Tariffs and Limits regarding payments cards issued by BC"Eurocreditbank" S.A. (hereinafter Tariffs and Limits)

General Banking Conditions, as the Tariffs and Limits are accessible on the information boards in the Bank's subdivisions and on the Bank's web page.

1.3. These Terms and Conditions govern the attachment, activation and use of eligible Bank-issued cards in Apple Pay.

1.4. The Bank allows the use of eligible cards issued by the Bank in Apple Pay applications in order to perform payment operations.

1.5. These Terms and Conditions govern the access and use of the card in Apple Pay applications only between the customer, as the cardholder, and the Bank.

1.6. Providers of devices through which payments can be made through Apple Pay applications or third parties with whom they collaborate may have their own terms and conditions.

1.7. These Terms and Conditions do not apply to services/products purchased from the provider of the device, mobile network, or from other pages, or services belonging to third parties that integrate or enable the provision of Apple Pay. The Bank is not responsible for the legality of the supply / performance of the products / services of the device supplier and / or of third parties, nor for the security, accuracy, legality or any other aspect of the respective products / services offered by them.

1.8. For additional information about Apple Pay, the cardholder can access the Apple Wallet and/or Apple Pay compartment on the [www.apple.com](http://www.apple.com) page.

## CHAPTER 2. Terms and definitions

### 2. Notions used

In the context of this document, the terms below will be understood as follows:

- Apple – Apple Distribution International based in Hollyhill Industrial Estate, Cork, Ireland

provider of Apple Pay.

- Apple Pay - (hereinafter service) is a mobile payment service by Apple Inc. that allows users to make payments in person, in iOS apps, and on the web. It is supported on iPhone, Apple Watch, iPad, and Mac. It digitizes and can replace a credit or debit card chip and PIN transaction at a contactless-capable point-of-sale terminal. It does not require Apple Pay-specific contactless payment terminals; it can work with any merchant that accepts contactless payments. It adds two-factor authentication via Touch ID, Face ID, PIN, or passcode. Devices wirelessly communicate with point of sale systems using near field communication (NFC), with an embedded secure element (eSE) to securely store payment data and perform cryptographic functions, and Apple's Touch ID and Face ID for biometric authentication. It can also be used to ride some public transport networks either through the use of credit/debit cards or dedicated travel cards.

- Apple Pay application – a payment platform offered by Apple Distribution International, via

which the user can attach eligible cards to make payments at merchants, pay online, withdraw cash at contactless ATMs via Apple devices.

- Card eligible for attachment and use in Apple Pay – payment debit and/or credit card

asset of the Visa Inc. international system, issued by the Bank in the name of the cardholder, in accordance with the contract concluded between the cardholder and the Bank.

- CVV2 – a 3-digit security code printed on the back of the card.
- Cardholder – person in whose name a debit and/or credit (primary, secondary or corporate) card is issued.

- Apple Pay compatible device – smartphone, tablet, smartwatch or other type of device that

allows payments to be made via Apple Pay. These devices are listed on [www.apple.com](http://www.apple.com).

- Find My iPhone – an application used to locate and protect devices such as: iPhone, iPad, Apple Watch, etc. in case of loss or theft.

- Face ID – facial recognition of the card holder, owner of the device and is based on secure authentication that allows the identification of the face geometry.

- FingerPrint – recognition of the fingerprint of the card holder, owner of the device.

- iCloud – the service that allows storing the content of Apple devices.

- One-time password (OTP) – the password generated and sent by the Bank to the cardholder (via the mobile phone operator with which the Bank has concluded a contract) in an SMS message to the phone number of the cardholder registered in the Bank's information systems.

- Electronic wallet – Apple Pay.

- Cardholder Verification – cardholder authentication procedure. When attaching the eligible card to the electronic wallet, verification of the holder is performed by entering the one-time password by the cardholder. The duration of the single-use password is limited and is determined by the Bank (30 minutes). The conditions, cases and frequency with which the password is requested to verify the cardholder when making transactions are established by the providers.

- Token – a unique series of digits in digital format that ensures secure substitution of the card's PAN.

- Tokenization – a process of replacing a confidential data element (PAN) with a non-confidential equivalent, called a token, which has no independent meaning/value for external or internal use and is used in the field of information security.

- Near Field Communication (NFC) – a standard used in the case of electronic devices through which a high-frequency radio communication is established that allows the wireless exchange of data over a very short distance, up to 10 centimeters each.

## CHAPTER 3. General Description of Apple Pay

3.1. The bank offers cardholders the possibility of attaching the card to Apple Pay by accepting the present Terms and Conditions.

3.2. To use the card in Apple Pay, the cardholder must have an Apple Pay compatible device.

3.3. The basic functionality of Apple Pay consists in making transactions through contactless technology by means of the payment card, tokenized in Apple Pay.

3.4. Apple Pay allows the attachment of up to 10 (ten) payment cards.

3.5. The bank offers the possibility to add a single card to a maximum of 10 Apple Pay devices at the same time. The device provider may impose limitations or restrictions and/or have minimum software and hardware requirements for the compatible device used.

3.6. To attach and use cards in Apple Pay, the cardholder must meet the following conditions:

3.6.1. have an Apple device, as indicated on the Apple page:  
[www.apple.com](http://www.apple.com).

3.6.2. the Apple device to which the card is to be attached must contain active NFC technology and the operating system indicated by Apple.

3.6.3. to have registered in the Bank's systems a mobile phone number that belongs to one of the operators in the Republic of Moldova.

3.6.4. to have at least one eligible card.

3.6.5. meet the conditions for registration as a user in Apple Pay and any other requirements established and/or requested by Apple for the use of the application, mentioned on the Apple page. The bank has no responsibility towards the cardholder regarding the requirements/conditions and/or any limitations/restrictions on the use of the application established by Apple, nor to their modification and/or communication to the cardholder.

3.7. The bank does not charge a commission or other payment for the use of cards in Apple Pay. The provider of the Apple Pay device and / or third parties may charge fees, impose limitations and restrictions that could affect the use of any Bank-issued card in Apple Pay. The customer is responsible for paying these fees and agrees to comply with any limitations or restrictions imposed.

#### CHAPTER 4. Attaching Eligible Card to Apple Pay

4.1. To attach the card to Apple Pay, the cardholder must meet at least the specific conditions for registering as a device user:

- have a compatible device.
  - to have an Apple ID account for the services offered by Apple, authenticated within the iCloud service.
  - set one of the ways to lock/unlock the screen on the device (password, fingerprint, Face ID).

4.2. The requirements mentioned in point 4.1 are conditions imposed by the application provider, the Bank has no responsibility in relation to the established requirements.

4.3. After meeting the above conditions, the cardholder:

- will access the Wallet application from the Apple device in the Apple application, which is subject to Apple's terms and conditions.
- will initiate the entry of card data: scan or manually enter the data in Apple Pay: name and surname, card number, expiration date, and enter the CVV2 code.
- will accept these Terms and Conditions that will be displayed in Apple Pay.
- will enter the verification code (OTP) in the application for authentication as the card holder. If the attachment request is rejected, the user can contact the Card Support Service to obtain information about this situation.

## CHAPTER 5. Use of Card/Token via Apple Pay

5.1. Attaching the card to Apple Pay generates the card token for making payments through Apple Pay. The token number is different from the card number attached in Apple Pay, this fact increases the security of transactions.

5.2. For each attachment of the same card on different Apple devices, a different token associated with that device will be generated.

5.3. The token generated in Apple Pay can be used to:

- Contactless payments at merchants - by bringing the device close to the merchant's payment terminal (eg POS). This action is performed by unlocking the mobile device through Fingerprint / Face ID / entering the password, in the case of the Apple Watch - by double-clicking on the side button of the device and bringing the device closer to the contactless reader.

- Pay on web pages that display the "buy with Apple Pay" option by typing the button when paying for the order. This action is performed by unlocking the mobile device through Fingerprint / Face ID / entering the password, in the case of

Apple Watch - by double clicking on the side button of the device, and confirming the transaction.

- Cash withdrawals at contactless ATMs. For cash withdrawal, it will be necessary to enter the PIN of the card on the ATM terminal where the withdrawal is made. This action is initiated by unlocking the mobile device through Fingerprint / Face ID / entering the password, in the case of the Apple Watch - by double-clicking on the side button of the device, and bringing the device closer to the contactless reader.

5.4. If the cardholder has attached more than one eligible card to Apple Pay, then the first card attached to the device will be selected by default when making payments. The card user has the possibility to change the card selected as default for payments in Apple Pay at any time.

5.5. Within the Apple Pay application, the provider will provide the cardholder with information on the last 10 transactions made with the token associated with the device.

5.6. When the validity period indicated on the front of the Card registered in Apple Pay expires, the service can only be used after registering the renewed Card in Apple Pay.

5.7. When the card is reissued, the related token will no longer be able to be used in Apple Pay. The service can only be used after registering the new Card in Apple Pay and assigning a new token.

5.8. If the payment card is blocked by the customer, Apple Pay payments will be available.

If the payment card will be blocked by the Bank or prohibition measures will be applied to the card account (suspension, seizure within the limit of the blocked amount, etc.) payments via Apple Pay will not be available.

5.9. All limits/conditions established for a payment card according to the General Banking Conditions and Tariffs and limits they are also valid for the card attached to Apple Pay.

## CHAPTER 6. Token Management (Locking/Unlocking) in Apple Pay

6.1. The token can be blocked/unblocked through the Card Support Service.

6.2. The blocked token can be unblocked by the Card Support Service depending on the token blocking status and only if the customer has been successfully identified.



6.3. The customer has the possibility to delete the card from the Apple Pay application from Apple Pay devices using the Find My Phone application, iCloud.com or directly from the electronic wallet.

Note: For additional information on how to delete the card from applications on Apple devices, the cardholder can visit [www.apple.com](http://www.apple.com). The customer can suspend the Apple Pay device by placing it in lost mode using the application in the phone settings - Find My Phone.

## SECTION 7. Termination of Use of Cards through Apple Pay

7.1. Stopping the use of the physical card by the cardholder does not automatically stop the possibility of using it for Apple Pay transactions.

7.2. The cardholder can stop using the application by removing the attached card from the Apple Pay application at any time. This fact will not influence the possibility of using the physical card.

7.3. In the event that the provider of the devices and/or of the Apple Pay application suspends, blocks, interrupts the use of the Apple Pay application and/or modifies its functionality, the possibility of using the cards in the Apple Pay application will be interrupted or modified accordingly

## CHAPTER 8. Apple Pay Security

8.1. The cardholder is obliged to ensure the confidentiality of the information recorded in the electronic wallets, to take protective measures and not to allow its use by third parties.

8.2. The cardholder is responsible for the use and transactions made with the card in the electronic wallets, including by third parties to whom the cardholder voluntarily or involuntarily provided access to the card/device, or to other security details.

8.3. To prevent unauthorized access, the Bank recommends applying the following measures:

- continuous keeping of the device safe and in the owner's possession;
- keeping security information and access passwords in maximum safety and not communicating them to other people;
  - setting security passwords in accordance with information security requirements;
- keeping cards in physical format and/or card details separately from the device used, etc.

8.4. Apple Pay may use certain Security features and procedures to protect against unauthorized use of any Card. These functionalities and procedures belong exclusively to the device provider.

8.5. Before entering the card data into the e-wallet, the cardholder will be asked to set the password/security details, which he will use to access them. The conditions, cases and frequency with which this password / security details are requested are set by the e-wallet providers.

8.6. The Bank is not responsible for the transactions made with the card issued by the Bank and attached to the electronic wallets until it is informed of the occurrence of a suspicious event or until the blocking of the token is requested.

8.7. Apple Pay may use certain security features and procedures to protect against unauthorized use of any card. These functionalities and procedures belong exclusively to the device provider. By attaching the card issued by the Bank to the e-wallets, the cardholder agrees not to disable any of the security features and to use them to protect all cards issued by the Bank and registered in the applications. The bank does not control these security methods and is not responsible for how Apple and / or the compatible device provider use them.

8.8. If the cardholder has detected that the mobile device, the Apple device, the card and/or other data have been compromised it is necessary to remove the card connected to Apple Pay.

## CHAPTER 9. Responsibilities of the parties

9.1. The Bank provides information about the transactions made with the cards issued by the Bank and attached to the electronic wallets in ways approved by the Bank (e.g. account statement, WEB Banking, etc.).

The transactions made will be displayed without indicating that they were made through the Apple Pay service.

9.2. The Bank has the right to block, restrict, suspend or terminate the possibility of using any card issued by the Bank in Apple Pay if these Terms and Conditions are violated or if any fraudulent or improper activity of the card in the applications is suspected.

9.3. The Bank is not responsible if the device provider imposes limitations or restrictions on the use of Apple Pay and/or may have minimum software and hardware requirements for the compatible device used.

9.4. The Bank shall not be liable to the Bank's cardholders who have attached their card to Apple Pay, in the event that the device and/or Apple Pay provider blocks, restricts, suspends or discontinues their use of Apple Pay.

9.5. The bank is not responsible and does not provide support or assistance for any hardware, software or other products or services of third parties. If you have any questions or problems with a product or service provided by Apple or a third party, you should contact the respective supplier / third party for assistance.

9.6. The bank is not responsible for access, use of the token created in Apple Pay, these depend on Apple Pay and the network of the Internet provider.

The Bank does not operate Apple Pay or such networks and has no control over their operations. The Bank will not be responsible for any situation that interrupts, prevents or otherwise affects the operation of any card issued by the Bank and attached to Apple Pay, such as, but not limited to, the unavailability of the Apple Pay service or the Internet service, communications, delays in network, internet coverage limitations, system outages.

9.7. The bank is not responsible for losses, moral or patrimonial damages caused by the client's non-compliance with these Terms and Conditions.

9.8. The bank is not responsible for damages resulting from the execution of unauthorized payments generated by the exposure of the cardholder's device to viruses and/or other applications/programs, as well as its theft.

9.9. The cardholder is responsible for:

- Confidentiality of one-time passwords, passwords, PIN code and other means of access to the mobile device, mobile application, card, token;
- Limiting access to the mobile device / Apple device, the existence and updating of antivirus programs installed on the mobile device;
- Disallowing the use by third parties of the mobile device on which the mobile application was installed;
- Operations performed using the Apple Pay service on the owner's device;
- Immediately informing the Bank about the need to block the card/token or delete the card/token;
- Removing the card from the mobile application before removing the mobile application from the mobile device;
- Removing the card before destroying the mobile device and before handing over the mobile device in use / property to a third party;
- Execution of instructions and work rules with the mobile application.

9.10. The cardholder has the obligation to:

- to take safety measures, to consult and respect the security conditions imposed by Apple, as well as to carry out all Apple indications to avoid unauthorized use of the token.
- attach your card to the Apple Pay application only on devices that you legally own, as well as take security measures to avoid unauthorized use of the token.

- to notify the Bank when the attached card and/or the device to which the card was attached was lost/stolen or used without its consent and to block the token associated with it according to chapter 7. Otherwise, the Bank will not be responsible for the payments made with the token in the event of the occurrence of any of the previously listed events.

- keep his credentials in Apple Pay and/or for his Apple ID account and/or for his device safe. The Bank is not responsible for token payments if these payments are made by other persons.

- to monitor the transactions made with the token and in case of any irregularities to immediately notify the Bank by calling the Card Support Service.

## CHAPTER 10. Final provisions

10.1. The Bank will inform the cardholders regarding the modification of the present Terms and Conditions of Use by displaying the modified version(s) of this document on the Bank's website ([www.ecb.md](http://www.ecb.md)) and the information panel in the Bank's subdivisions.

10.2. If there is any inconsistency between the terms of Apple Pay Connect and these Terms and Conditions, the present Terms and Conditions will apply for transactions made with the card issued by the Bank in Apple Pay.

10.3. The cardholder can contact the Bank through the Card Support Service at phone number +373 22 50-02-20 for any problem related to attaching, blocking/unblocking, deleting a card or executing card payments in electronic wallets.

10.4. This document enters into force on 12.06.2023.