Simbank

ААКнын Башкармасы тарабынан
БЕКИТИЛДИ
“25” июль 2024-жылдагы
№ 39 протокол

“Дос-Кредобанк” ААКнын Visa “Simbank”
банктык төлөм карталарын коопсуз пайдалануу эрежелери

Картаны жокко чыгаруу — картаны жараксыз деп таануу жана аны жүгүртүүдөн алып коюу.

OTP – One Time Password (бир жолку пароль)

Банк – “Дос-Кредобанк” ачык акционердик коому

Банк-эмитент — картаны чыгарган, ошондой эле башка банктардын – төлөм системасынын катышуучуларынын алдында милдеттенмелер боюнча жооп берген, банк, төлөм системасынын катышуучусу.

Банк-эквайер — эквайринг жүргүзүүгө уруксат алган банк, аралыктагы жабдуулар тармагынын ээси. Тиешелүү төлөм системаларынын технологияларына жана ченемдик актыларына жана Кыргыз Республикасынын мыйзамдарына ылайык өзүнүн аралыкта орнотулган жабдуулары аркылуу авторизациялоону же транзакцияларды жүргүзүүнү камсыз кылат.

Банктык эсеп (мындан ары карт-эсеп) — акча каражаттарынын жылышы жана карта боюнча транзакцияларды жүргүзүү үчүн карта ээсине банк тарабынан ачылган эсеп.

Банкомат — накталай акчаны берүү жана кабыл алуу, картага акча каражаттарын салуу, жүргүзүлгөн транзакциялар боюнча маалыматты алуу, накталай эмес төлөмдөрдү жүргүзүү жана транзакциялардын бардык түрлөрү боюнча карт-чекти алуу үчүн аппарат. Банкомат банктын кызматкерлери катышпаган, карта менен өз алдынча операциялар үчүн арналган. Мындан ары ATM – Automatic Teller Machine катары кездешет.

Картаны блоктоо — карта боюнча операцияларды жүргүзүүгө толук же убактылуу тыюу салуу.

Банкоматтык көчүрмө — карта ээсинин суроо-талабы боюнча банкомат тарабынан түзүлгөн карт-эсеп боюнча көчүрмө. Банкоматтан көчүрмө карт-эсеп боюнча жүргүзүлгөн максимум 10 (он) акыркы транзакцияны камтыйт.

Банктык төлөм картасы— (мындан ары текст боюнча карта) товарларга, иштерге жана кызматтарга төлөө, которуулар жана башка төлөмдөрдү жүргүзүү үчүн, ошондой эле накталай акча алуу үчүн төлөм куралы. Карта анда көрсөтүлгөн мөөнөт ичинде гана жарактуу. Мөөнөтү өтүп кеткен карталар боюнча операциялар жүргүзүлбөйт.

Карта ээси — банктык тейлөө келишиминин шарттарына ылайык картаны пайдаланууга укуктуу жеке адам.

Лимит(тер) — карта боюнча операциялардын максималдуу суммасына карата банк тарабынан белгиленген чектөөлөр. Лимит(тер) бир операциянын суммасына жана валютасына карата, ошондой эле белгилүү бир убакыт аралыгында жүргүзүлгөн бардык операциялардын суммасына карата белгилениши мүмкүн.

Алдамчылык операция — санкцияланбаган жана карта ээси тарабынан тастыкталбаган карта боюнча операция.

Штаттан тышкаркы кырдаал — төлөм системасынын киргизилген автоматтык каражаттары менен чечилбей турган жана персонал тарабынан атайын уюштурулган ишти талап кылган кырдаал.

ПИН-код — жеке идентификациялык номер, картаны пайдалануу үчүн жашыруун код. Карта ээси “Simbank” тиркемесинде ПИН-кодду өзү белгилейт. ПИН-код төрт сандан турат.

Шектүү операция (бүтүм) – төмөнкүдөй белгилерди камтыган операция (бүтүм):
а) эгерде каражаттар кылмыштуу жол менен, анын ичинде предикаттык кылмыштан алынган киреше экенине же кылмыштуу кирешени легалдаштырууга (адалдоого) байланыштуу экенине шектенүү болсо же шектенүүгө жетиштүү негиздер болсо;
б) эгерде каражаттар төмөнкүлөрдү каржылоо менен байланыштуу экенине шектенүү болсо же шектенүүгө жетиштүү негиздер болсо:
- террористтер жана экстремисттер;
- террористтик жана экстремисттик уюмдар (топтор);
- террористтик жана экстремисттик иш.

ПОС-терминал — картаны же аралык төлөмдөрүнүн куралдарын пайдалануу менен соода-тейлөө ишканаларында товарлар жана кызматтар үчүн төлөмдөрдү кабыл алуу үчүн түзүлүш.

Террористтик ишти каржылоого жана кылмыштуу кирешелерди легалдаштырууга (адалдоого) каршы аракеттенүү – террористтик ишти каржылоого жана кылмыштуу кирешелерди легалдаштырууга (адалдоого) каршы аракеттенүүгө, ошондой эле экстермисттик ишти каржылоого жана жалпы кыргын салуучу куралды жайылтууну каржылоого каршы аракеттенүүгө багытталган чаралар комплекси.

Стоп-барак — банк-эмитент төлөм каражаты катары кабыл алууга тыюу салган карталардын тизмеси.

Эсеп боюнча көчүрмө — карт-эсептеги акча каражаттарынын калдыгы жөнүндө, көрсөтүлгөн мезгилде карт-эсеп боюнча акча каражаттарынын жылышы жана карта боюнча операциялар жөнүндө отчет.

Транзакция — жыйынтыгында транзакциянын суммасына карт-эсепти дебеттөө же кредиттөө жүргөн карта боюнча операция (товарларды же кызматтарды сатып алуу, валюталарды алмашуу же накталай алуу).

Техникалык овердрафт — чыгыштоо операцияларынын суммасы карт-эсептеги жеткиликтүү калдыктан жогору болгондо пайда болуучу карыз.

CVV2-код — Интернет аркылуу төлөөдө жана башка операция түрлөрүндө картанын аныктыгын текшерүү үчүн үч орундуу код. Аны картанын арткы тарабынан табууга болот.

3D Secure — Интернетте карталар боюнча төлөмдөрдүн коопсуздугун камсыздоо үчүн заманбап технология. 3D Secure паролду киргизүү аркылуу карта ээсин кошумча идентификациялоого жана алдамчылык тобокелдигин максималдуу азайтууга мүмкүнчүлүк берет.

1. **Жалпы жоболор**

1.1. Карталарды чыгаруу жана тейлөө боюнча карта ээси менен банктын ортосундагы укуктук мамилелер Жеке жактарга банктык кызматтарды көрсөтүү жөнүндө айкын оферта келишими (мындан ары текст боюнча – Келишим) менен жөнгө салынат.
1.2. Картаны башка адамдарга пайдаланууга же күрөө катары берүүгө тыюу салынат. Ыйгарым укуксуз адам тарабынан көрсөтүлгөн карта алынып коюлат.
1.3. Карта Банктын менчиги болуп саналат, картанын, Келишимдин колдонуу мөөнөтү аяктаганда же Банктын биринчи талабы боюнча карта милдеттүү тартипте Банкка кайтарылышы керек.
1.4. Ушул эрежелер жана тарифтер Банктын расмий сайтында жайгаштырылат Simbank.kg
1.5. Банк расмий сайтта жаңы редакцияны жайгаштырып, ушул эрежелерди бир тараптуу тартипте өзгөртүүгө укуктуу.
1.6. Банк FATCA мыйзамынын талаптарынын алкагына АКШнын салыктык резиденттери боюнча АКШнын салык органдарына маалымат берүүгө укуктуу.

2. **ПИН-кодду пайдалануу**

2.1. Картаны алгандан кийин карта ээси аны картанын акыркы 8 цифрасын киргизүү аркылуу “Simbank” мобилдик тиркемесинде активдештирет.

2.2. Simbank мобилдик тиркемесинде картаны ийгиликтүү активдештирүүдөн кийин, картанын ПИН-коду мобилдик тиркеме менен окшош болот.

2.3. ПИН-кодду алмаштыруу банктын мобилдик тиркемесинде карта ээси тарабынан жүргүзүлөт.

2.4. Карта ээси ПИН-код үчүн 4 цифрадан турган комбинацияны өзү тандайт. Карта ээси ачык-айкын, оңой божомолдонуучу цифралар комбинациясын пайдаланбашы керек, мисалы, телефон номеринин акыркы цифралары, туулган күн ж.б.

2.5. ПИН-кодду терүүдө электрондук түзүлүштөрдүн дисплейинде цифралар атайын көрсөтүлбөйт, шарттуу белги менен алмаштырылат. Терүүдө катага жол бербеш керек. Эгерде үч жолу катары менен (каалаган убакыт аралыгында) туура эмес ПИН-код берилсе, карта автоматтык түрдө блоктолот. Кардар картада көрсөтүлгөн 7700 телефон номери боюнча Банктын колдоо кызматына кайрылышы керек.

2.6. ПИН-код менен ырасталган карта операцияларын банк карта ээси тарабынан жүргүзүлгөн катары кабыл алат.

3. Картаны колдонуу.

Картаны төмөнкүлөр үчүн колдонууга болот:

- Соода-тейлөө ишканаларында нактадай эмес формада товарларга жана кызматтарга төлөө.
- Банктын бөлүмдөрүндө жана банкоматтар аркылуу накталай акча алуу.
- Интернет тармагында операцияларды жүргүзүү.

4. Соода-тейлөө ишканаларында карта менен төлөө.

4.1. Карталар тейленген бардык пункттар VISA TC логотиби бар маалыматтык көрсөткүчтөр менен жабдылган.

4.2. Товарларга же кызматтарга төлөө үчүн соода түйүнүнүн кызматкерине картаны көрсөтүү керек.

4.3. Коопсуздук жана жеке маалыматтарды коргоо максатында соода-тейлөө ишканаларында картаны пайдалануу менен бардык транзакциялар карта ээсинин катышуусунда жүргүзүлүшү керек.

4.4. Айрым соода жана тейлөө уюмдарында ири сатып алууларда өздүк күбөлүктү сурашы мүмкүн. Ошондуктан карта менен төлөөдө банк жаныңызга паспортту же өздүгүн күбөлөндүргөн башка документти алууну сунуштайт.

4.5. Карта менен төлөөдө авторизациялоо ПОС-терминалдын жардамы менен жүргүзүлөт. Кассир клавиатурада операциянын суммасын терет. Андан кийин кассир (же карта ээси өзү) картаны ПОС-терминалдын окуучу түзүлүшүнө коёт же картаны ПОС-терминалда байланышсыз чип-ридерге жакындатат. Суроо-талап байланыш каналдары аркылуу банкка түшөт. Эгерде карта ээси туура ПИН-кодду тандаса жана картада жетиштүү акча болсо, транзакцияны жүргүзүүнү тастыктаган чек эки нускада басылып чыгат. Карта ээсине чектин бир нускасы берилет. Чектеги маалыматтарды текшерүү керек. Колдонулган технологияга жараша басылып чыккан чек карта ээсинин жана кассирдин кол тамгалары менен күбөлөндүрүлөт.

4.6. Эгерде анда картадан алына турган операциянын суммасы жазылбаса, дата (же операциянын башка деталдары) жок болсо, чекке кол коюуга тыюу салынат. Эгерде карта ээси көрсөтүлгөн маалыматтарда так эместиктерди аныктаса, кол коюудан баш тартып, операцияны жокко чыгарып жана жокко чыгаруу жөнүндө чекти сураш керек.

4.7. Банк сатып алгандан кийин чектерди сактоону сунуштайт. Алар талаштуу маселелер жана карт-эсептен каражаттарды алууда так эместиктер пайда болгон учурда керек болот.

5. Интернет тармагында карта менен төлөө.

5.1. Интернетте карта менен төлөө үчүн анын реквизиттери колдонулат: карта номери, колдонуу мөөнөтү, карта ээсинин аты. Айрым сайттар CVV2 жана 3D Secure пароль сыяктуу реквизиттерди кошумча сурашы мүмкүн.

5.2. 3D Secure жана Интернетте төлөөгө жетүү мүмкүндүгү алдын ала бардык VISA карталары үчүн ачык.

5.3. Мүмкүн болгон тобокелдиктер үчүн, мисалы, үчүнчү жактардын карта боюнча санкцияланбаган интернет-төлөмдөрдү жүргүзүүсү үчүн жоопкерчилик карта ээсине жүктөлөт. Мында банк карта ээсинен арыздарды кабыл алат (акча каражаттарын кайтарууга жана/же мындай операциялар боюнча дооматтык ишти) жана колдонуудагы ЭТС эрежелерине ылайык иштеп чыгат.

5.4. CVV2 коду — бул картанын арткы тарабында басылган үч орундуу код.

5.5. Банк белгилүү компаниялардын текшерүүдөн өткөн сайттарында гана сатып алууну сунуштайт.

5.6. Ошондой эле банк 3D Secure коопсуздук технологиясын кармаган сайттарда төлөмдөрдү жүргүзүүнү сунуштайт.

5.7. 3D Secure технологиясы боюнча операцияларды жүргүзүүдө карта ээси картаны чыгарууда ал көрсөткөн номерге келген СМС-билдирүүдөгү/push-билдирүүдөгү паролду киргизиши керек. Бул пароль бир жолку болуп саналат.

5.8. Интернет тармагындагы коопсуз операциялар үчүн карта ээси аткарышы керек:

- Браузерин жана вируска каршы программаларды өз убагында жаңыртуу.
- Картанын колдонуу мөөнөтүн, блоктоо бар-жогун ж.б. текшерүү.
- Картада төлөмдү жүргүзүү үчүн акча жетиштүү экенин текшерүү.
- Автоматтык түрдө багытталган баракчаларда же калкыма терезелерде операцияларды жүргүзүүдөн алыс болуу.
- Төлөө жана буйрутманы ырастоо үчүн сайттын көрсөтмөлөрүн так сактоо.

5.9. Төлөмдү жүргүзүүдөгү баш тартуунун мүмкүн болуучу себептери:

- Картада каражаттар жетишсиз.
- Картада Интернет тармагында төлөмдөргө тыюу салынган же башка чектөөлөр орнотулган.
- Картанын колдонуу мөөнөтү аяктаган.
- Карта ээси 3D Secure паролду көрсөткөн эмес.
- Карта блоктолгон.
- Банк тарабынан шектүү операцияларды жүргүзүүгө тыюу салынган.
- Картаны ачууда туура эмес/жоголгон телефон номери көрсөтүлгөн жана 3D Secure коду бар билдирүү туура эмес номерге келет.
- Сайт же сайт санкцияга алынган жана өтө тобокелдиктүү деп эсептелет.
- Браузерлер тарабынан cookie уруксат берилген эмес.
  Баш тартуунун себебин аныктоо үчүн карта ээси банкка кайрыла алат.

5.10. Төлөмдү толук же жарым-жартылай жокко чыгаруу үчүн карта ээси Интернет-дүкөндүн колдоо кызматына кайрылышы керек.

5.11. Карта ээси Интернет аркылуу карта боюнча төлөмдөрдү жүргүзүүнү өз алдынча блоктой алат. Бул үчүн Simbank тиркемесинде лимиттер бөлүмүндө 0 (нөл) лимитин коюу керек.

6. Банкоматта накталай акчаны алуу.

6.1. Банкоматты колдонуудан мурда шектүү түзүлүштөрдүн бар экенин текшерүү зарыл: тегиз эмес орнотулган клавиатура, банкоматтын экранынын үстүндөгү койгучтар ж.б. Мындай түзүлүштөр аныкталган учурда банкоматта операцияларды жүргүзүүдөн алыс болуу жана мүмкүн болушунча банкоматта көрсөтүлгөн телефон аркылуу же банктын Колл-борборуна чалуу аркылуу банк кызматкерлерине шектенүүлөрүңүз тууралуу билдирүү керек.

6.2. Банкоматта накталай акча алуу үчүн карта ээси ПИН-код киргизет жана банкоматтын экранындагы нускаманы аткарат.

6.3. Операцияны “Жокко чыгаруу” / “Cancel” баскычынын жардамы менен жокко чыгарууга болот.

6.4. ПИН-кодду терүүдө аны башка адамдар көрбөгөнүн текшерүү керек. Эгерде үч жолу туура эмес ПИН-код киргизсеңиз, карта блоктолот. Картаны блоктон чыгаруу үчүн 7700 номери же Telegram, WhatsApp мессенджерлери аркылуу банктын колдоо кызматына кайрылуу керек.

6.5. Коопсуздук максатында банкоматта бардык операцияларды үчүнчү адамдардын жардамысыз өз алдынча жүргүзүү керек.

6.6. Ар кандай банктардын банкоматтарында накталай акча алуу үчүн бир жолку лимит айырмаланышы мүмкүн.

6.7. Банкомат аркылуу алынган квитанцияларды сактоону сунуштайбыз, анткени алар ПИН-код менен тастыкталган жана бүтүмдү ырастоо болуп саналат.

6.8. Экранда “Картаңызды алыңыз” деген жазуу пайда болгондон кийин, картаны дароо алуу керек, болбосо ал банкомат тарабынан алынып коюлат.

6.9. Банкомат тарабынан берилген акчаны 20 (жыйырма) секунданын ичинде алуу керек, болбосо коргоо системасы иштейт жана банкомат аны кайра алып коёт. Бул коопсуздук максатында каралган.

6.10. Эгерде банкомат картаны же акчаны алып койсо, дароо кетпеш керек, бир аз убакыт күтүш керек. Балким бул техникалык мүчүлүштүк болгон жана банкомат картаны же акчаны кайтарып берет, ал эми карта ээси кетип калган болот.

6.11. Банкоматта операцияларды жокко чыгаруунун мүмкүн болгон себептери:

- банкоматта сураган суммага ылайыктуу банкноттор жок. Банкоматта көрсөтүлгөн банкноттордун минималдуу номиналынын эселенген сумманы сураш керек.
- Сураган сумма банкоматтын габариттери менен аныкталган бир жолку берүү лимитинен ашып кетет. Суралган сумманы бөлүктөргө бөлүп, операцияны бир нече жолу кайталоого болот.
- Суралган сумма картадагы акча калдыгынан ашып кетет. Картадагы калдыкты билүү үчүн банкоматтын менюсундагы мындай опцияны колдонсоңуз болот.
- Банкоматтан накталай акча алып жатканда банкомат керектүү төлөм системасынын картасын тейлей турганын текшериңиз (негизинен банкоматтарда банкомат тейлеген төлөм системаларынын логотиптери бар).

7. Картаны жоготкондо/уурдатканда.

7.1. Картаны жоготкон же уурдаткан учурда, ошондой эле картаны ыйгарым укуктуу эмес адамдын пайдаланганына шектенүүлөр болсо, тез арада банкка кайрылуу зарыл, банктын оператору картаны дароо блоктойт, карта ээси банктын тиркемеси аркылуу картаны өз алдынча блоктой алат. Мында карта ээси блоктогондон кийин Simbank тиркемесинде төлөмдөрдү жана Google Pay/Garmin Pay аркылуу сатып алууларды жүргүзө алат.

7.2. Картаны, ошондой эле Simbank аккаунту бар смартфонду жоготкон же уурдаткан учурда карта ээси банктын колдоо кызматына кайрылып, картаны блоктоого тийиш: 7700 номери же Telegram, WhatsApp мессенджерлери аркылуу.

7.3. Карта ээси картаны блоктоого чейин жүргүзүлгөн карта операциялары үчүн жоопкерчилик тартат жана блоктоо учурунан тартып мындай жоопкерчиликтен бошотулат.

7.4. Эгерде карта ээси картаны жоготкондугу же уурдаткандыгы жөнүндө арыз бергенден кийин аны тапса, бул тууралуу банкка билдирүү зарыл. Эгер ээси бул картаны мындан ары колдонууну кааласа, картаны блоктон чыгаруу үчүн банкка кайрылышы керек.

7.5. Банк карта боюнча санкцияланбаган транзакциялар жүргүзүлбөгөнүн текшерүү үчүн кийинки айларда карт-эсеп боюнча көчүрмөнү текшерүүнү сунуштайт.

8. Төлөм системасындагы штаттан тышкаркы кырдаалдар.

8.1. Төлөм системасында төмөнкүдөй штаттан тышкаркы кырдаалдар жаралышы мүмкүн: электр менен жабдуунун үзгүлтүк болушу; байланыш каналдарындагы үзгүлтүк; системанын аппараттык жана программалык камсыздоосунун үзгүлтүк болушу; форс-мажордук жагдайлар (өрт, суу ташкыны, жер титирөө ж.б.).

8.2. Банк карта операцияларына катышкан жабдуулардын жана системалардын үзгүлтүксүз иштөөсүн камсыз кылуу үчүн бардык мүмкүн болгон чараларды көрөт.

9. Карта боюнча шектүү операциялар.

9.1. Эгерде Банк карта менен алдамчылык (мүнөздүү эмес), шектүү аракеттер жасалып жатат деп шектенсе, ал карта ээсинен кошумча маалыматтарды жана документтерди талап кылууга укуктуу. Карта ээси белгиленген мөөнөттө суралган документтерди, маалыматтарды бербеген же туура эмес документтерди берген учурда, Банк операцияны четке кагууга жана/же карт-эсепти андан ары жабуу менен картаны блоктоого укуктуу.

9.2. Банк террористтик ишти каржылоого жана кылмыштуу кирешелерди легалдаштырууга (адалдоого) каршы аракеттенүү (мындан ары текст боюнча – ТИКК) боюнча Кыргыз Республикасынын мыйзамдарынын чегинде тыюу салынган сайттарда, мыйзамсыз кызмат көрсөтүүлөрдү/товарларды, онлайн-казино боюнча операцияларды сунуштаган сайттарда, букмекердик сайттарда, чоңдор үчүн контентти камтыган сайттарда жүргүзүлгөн операцияларды жана башка төлөмдөрдү блоктоого/четке кагууга укуктуу.

9.3. Карта ээси Кыргыз Республикасынын мыйзамдарында тыюу салынган операцияларды жана Кыргыз Республикасынын террористтик ишти каржылоого жана кылмыштуу кирешелерди легалдаштырууга (адалдоого) каршы аракеттенүү жөнүндө мыйзамына туура келген операцияларды жүргүзбөөгө тийиш.

9.4. Банк алдамчылык жана шектүү операцияларга мониторинг жүргүзүүгө, карта ээсинен эсеп боюнча операцияларды жүргүзүү үчүн зарыл болгон, жүргүзүлүп жаткан операциянын мыйзамдуулугун жана экономикалык жактан максатка ылайыктуулугун жана кардардын реалдуу экономикалык ишти жүргүзүүсүнүн аныктыгын тастыктаган документтерди талап кылууга укуктуу.

9.5. Эгерде карта ээси карт-эсеп боюнча көчүрмөдөн талаштуу операцияны аныктаса, ал майда-чүйдөсүн тактоо үчүн банктын кызматкерине кайрылышы керек. Картадагы акчаны уруксатсыз пайдаланган учурда, карта ээси акчаны кайтарып берүү үчүн дооматтык арыз бериши керек. Бул үчүн 7700 номери боюнча же Telegram, WhatsApp мессенджерлеринде банктын колдоо кызматына кайрылуу керек.

9.6. Карта ээси операция жүргүзүлгөн учурдан тартып 45 (кырк беш) календардык күндүн ичинде дооматтык арызын бере алат. Бул мөөнөт аяктагандан кийин банк арызды кабыл албай коюуга укуктуу.

9.7. Талаштуу кырдаалды чечүү төмөнкүдөй жүргүзүлөт: банк дооматтык операция боюнча иликтөө жүргүзөт. Мында банк операциянын жүргүзүүнү тастыктаган кошумча документтерди (төлөө жөнүндө чек, АТМда акча алынгандыгы жөнүндө чек) талап кылууга укуктуу. Эгерде акча туура эмес алынгандыгы жана карта ээсинин күнөөсү жок экендиги тастыкталса, банк каражатты картага кайтарып берет. Дооматты карап чыгуу жана чечим кабыл алуу 3 (үч) айга чейин созулушу мүмкүн.

10. Коопсуздук эрежелери жана алдамчылык менен күрөшүү.

10.1. Банк карта ээсинин картаны пайдалануу боюнча коопсуздук эрежелерин сактабагандыгынан улам келип чыккан анын чыгымдары үчүн жоопкерчилик тартпайт.

10.2. Картаны үчүнчү жакка берүүгө тыюу салынат. Банк картаны үчүнчү жактын пайдалануусун одоно бузуу катары кабыл алат. Бул банктын демилгеси менен келишимди бузууга алып келиши мүмкүн.

10.3. Картаны обочо жерде сактаңыз. Картаны кимдир бирөө колдонуп же реквизиттерин (картанын номери, кол тамгасынын үлгүсү, CVV-код ч-код жана башка маалыматтар) көчүрө турган жерлерде калтырбоо керек.

10.4. Магниттик тилкени бузбоо үчүн картаны электромагниттик нурлануу булактарынын (уюлдук телефондор, сыналгылар, СВЧ-мештер, аудио жана видео аппаратура ж.б.) жанында кармабаңыз. Товарларды магниттик коддоо колдонулган жерлерде эсептешүүдө этият болуңуз – бул банкоматтарда жана ПОС-терминалдарда картаны иштеп чыгуудан баш тартууга же туура эмес иштеп чыгууга алып келиши мүмкүн.

10.5. Үчүнчү жактарга картанын ПИН-кодун бербеңиз. ПИН-кодду киргизүү менен жүргүзүлгөн операциялар карта ээси тарабынан жүргүзүлгөн катары таанылат жана талашууга жатпайт.

10.6. ПИН-кодду картанын өзүнө же картанын жанында сакталган документтерге жазбаңыз.
10.7. Соода кылууда картаны көрбөй калбагандай болуңуз. Транзакция аяктагандан кийин дароо картаны алыңыз.
10.8. Соода түйүндөрүндө карта менен болгон бардык операциялар карт ээсинин катышуусунда жүргүзүлүүгө тийиш.
10.9. Банкоматта операция жүргүзүүдөн мурун анын бузуктугунун тышкы белгилери барбы текшериңиз. Банкоматтын жанында же банкоматта бөтөн же шектүү жабдуулар табылганда, бул тууралуу банкоматты тейлеген банкка кабарлаңыз, андан кийин башка банкоматты колдонуңуз.
10.10. Экранында башка банкоматтарга өтүү тууралуу өтүнүч менен билдирүү көрсөтүлгөн банкоматтарды колдонуу сунушталбайт. Банктар мындай билдирүүлөрдү жарыялашпайт.
10.11. Жакшы жарыктандырылган жана ыңгайлуу жерлердеги банкоматтарды тандаңыз. Транзакция жүргүзүүдө жаныңызда эч кандай бөтөн адамдар жок экендигин текшериңиз.
10.12. Кийин чыгымдарды контролдоо үчүн бардык чектерди сактоо жана чектерди коомдук жайда таштанды контейнерине ыргытпоо сунушталат.
10.13. Шектүү сайттарда картанын реквизиттерин киргизүүгө болбойт. Болбосо, акчаңызды уурдап кетүү тобокелдиги жаралат.
10.14. ПИН-кодду киргизгенде, аны эч ким көрбөгөнүн текшериңиз.
10.15. Банк ар дайым карта ээсине карта боюнча бардык транзакциялар жөнүндө Simbank тиркемесинде Push-билдирүүнүн жардамы менен кабарлап турат.
10.16. Банкка берген байланыш маалыматыңызды өз убагында жаңыртып туруңуз. Мындай жол менен банк карта боюнча шектүү операция болгон учурда сиз менен дайыма байланыша алат.
10.17. Интернеттеги коопсуздук эрежелерин сактаңыз. Электрондук почтага же социалдык медиага шектүү же түшүнүксүз билдирүүлөр менен жөнөтүлгөн шилтемелерди баспаңыз. OTP паролду үчүнчү жактарга бербеңиз.
10.18. Электрондук почтадан сиз күтпөгөн шектүү файлдарды жүктөп албаңыз.
10.19. Паролуңузду жана жеке маалыматыңызды— телефон аркылуу, жеке же кат алышуу аркылуу эч кимге бербеңиз.
10.20. Сизди багыттап жаткан сайттардын даректерин (URL) кылдат талдаңыз. Көбүнчө алдамчылык сайты чыныгы сайтка окшош болуп көрүнөт, мында URL-дареги түп нускадан айырмаланат (мисалы, .gov ордуна .com менен аяктайт).
10.21. Браузериңизди жана коопсуздук программаларын өз убагында жаңыртып туруңуз.

15. Карта боюнча чектөөлөр.

15.1. Коопсуздук максатында банк карта операцияларына чектөөлөрдү белгилөөгө укуктуу. Лимиттердин өлчөмүн, ошондой эле аларды белгилүү шарттарын, мөөнөттөрүн жана тартибин банк өз алдынча аныктайт.
15.2. Банк алдамчылыкка жана терроризмди каржылоого жана кылмыштуу кирешени легалдаштырууга каршы аракеттенүүнүн алкагында карта операцияларына чектөөлөрдү киргизүүгө укуктуу, эгерде:
15.2.1 карта ээсинин же операциянын катышуучуларынын ичинен кимдир бирөөнүн маалыматтары алардын террористтик жана экстремисттик ишке, жапырт кыргыз салуучу куралдарды жайылтууга жана кылмыштуу кирешелерди легалдаштырууга (адалдоого) жана башка мыйзамсыз аракеттерге катышкандыгы жөнүндө маалыматтар бар жеке жана юридикалык жактардын, топтордун жана уюмдардын тизмесинде көрсөтүлсө;
15.2.2. карта ээси же операциянын катышуучуларынын ичинен кимдир бирөө ФАТФ сунуштамаларын сактабаган жана/же жеңилдетилген салыктык режимди берген жана/же финансылык операцияларды жүргүзүүдө маалыматты толук ачыкка чыгарбаган жана бербеген же ага карата эл аралык санкциялар колдонулган, жогорку тобокелдиктүү өлкөдө (мамлекет/аймак) катталса.
15.3. Банк тарабынан белгиленген стандарттуу чектөөлөр карта ээсинин банкка жазуу жүзүндө кайрылуусу боюнча өзгөртүлүшү мүмкүн.

15.4. Ошондой эле банк ПИН-код менен тастыкталбаган карта (NFC) боюнча байланышсыз төлөмдөрдүн суммасына чектөө киргизе алат.

16. Картанын колдонуу мөөнөтү жана келишимди бузуу.

16.1. Картанын колдонуу мөөнөтү (ай жана жыл) картанын өзүндө көрсөтүлгөн. Карта анда көрсөтүлгөн айдын акыркы күнүнө чейин жарактуу. Бардык мөөнөтү өтүп кеткен карталар блоктолот жана банкка тапшырылууга тийиш.

16.2. Карта ээси картаны жокко чыгарууга арыз берип, бир тараптуу тартипте картаны жабууга жана келишимди бузууга укуктуу.

16.3. Банк карта ээси келишимдин шарттарын жана эрежелерин аткарбаганда картаны блоктоого/жокко чыгарууга жана аны менен келишимди бузууга укуктуу.

16.4. Келишимди бузууда карта ээси карызды төлөөгө жана картаны тапшырууга тийиш.

16.5. Тараптардын биринин демилгеси боюнча келишимди бузууда жылдык тейлөө үчүн комиссия жана карта ээси төлөгөн башка комиссиялар кайтарылбайт.

16.6. Карта-эсеби боюнча акча каражаттарынын калдыгы банктын алдында карызы жок болгондо карта ээсине берилет.

17. Башка шарттар.

17.1. Карта ээси 5 (беш) күн ичинде картаны тариздөөдө ал документтерде көрсөткөн маалыматтардагы бардык өзгөрүүлөр жөнүндө банкка билдирүүгө милдеттүү. Эгерде карта ээси билдирбесе, банк пайда болушу мүмкүн болгон кесепеттер үчүн жоопкерчилик тартпайт.