Treasury and Trade Solutions

Security Procedures
Процедуры безопасности
Қауіпсіздік рәсімдері

1. Introduction
Введение
Кіріспе

These "Security Procedures", as referenced in the Communications section of the Master Account and Service Terms ("MAST") (or other applicable account terms and conditions), are designed to authenticate the Customer's log-on to the Bank's connectivity channels and to verify the origination of Communications between Bank and Customer in connection with the following Services or connectivity channels (the availability of which may vary across local markets).

Настоящие Процедуры безопасности, как установлено в Разделе "Сообщения" Общих условий ведения Счета и оказания Услуг ("Общие условия") (или других применимых условий обслуживания счетов), разработаны для подтверждения подлинности регистрации Клиента в каналах связи Банка и подтверждения происхождения Сообщений между Банком и Клиентом в отношении следующих Услуг или каналов связи (доступность которых может отличаться в зависимости от условий местных рынков).

Осы Қауіпсіздік рәсімдері, Шот жүргізу және Қызмет көрсету туралы жалпы шарттардың («Жалпы шарттар») (немесе шоттарға қызмет көрсетудің өзге қолданылатын талаптарына) «Хабарламалар» Тарауында келтірілгендей, келесе Қызметтер немесе байланыс каналдарына қатысты Клиентті Банктің байланыс каналдарында тіркелгенін растау үшін және Банк пен Клиент арасындағы Хабарламалардың шыққан жерін растау үшін (олардың қолжетімділігі жергілікті нарықтардағы талаптарға байланысты өзгеруі мүмкін) әзірленген.

- CitiDirect® (including WorldLink®)
  CitiDirect® ((включая WorldLink®)
  CitiDirect® (WorldLink® қоса)
- CitiConnect®
  CitiConnect®
  CitiConnect®
- Society for Worldwide Interbank Financial Telecommunication ("SWIFT")
  Общество всемирных межбанковских финансовых каналов ("SWIFT")
  Бүкіл әлемдік банк аралық қаржы каналдары қоғамы ("SWIFT")
- Manual Initiated Funds Transfer ("MIFT")
  Платежная инструкция на бумажном носителе ("MIFT")
  Қағаз тасымалдаушы нысанындағы төлем нұсқаулығы ("MIFT")
- Interactive Voice Response ("IVR")
  Интерактивный речевой ответ ("IVR")
  Интерактивтік ауызша жауап ("IVR")

- Email/Fax/Mail/Messenger/Phone with the Bank
  Электронная почта/факс/почта/мессенджер/телефон с Банком
  Электронды пошта/факс/пошта/мессенджер/Банкпен телефон
- Other local electronic connectivity channels
  Другие местные электронные каналы связи
  Басқа жергілікті байланыс каналдары

These Security Procedures are to be read together with the MAST and may be updated and advised to the Customer from time-to-time by electronic or other means, including but not limited to posting updates to the Security Procedures on CitiDirect. Unless otherwise provided by law, Customer's continued use of any of the above noted Services or connectivity channels after being advised of updated Security Procedures shall constitute Customer's acceptance of such updated Security Procedures. These Security Procedures cover the following:

Настоящие Процедуры безопасности должны читаться совместно с Общими условиями и могут время от времени пересматриваться и доводиться до сведения Клиента с помощью электронных средств связи или иным образом, включая, но не ограничиваясь публикацией обновленных Процедур безопасности на CitiDirect. Если иное не предусмотрено законодательством, использование Клиентом любой из вышеперечисленных Услуг или каналов связи после того, как он будет проинформирован о пересмотре и обновлении Процедур безопасности, будет считаться принятием таких пересмотренных Процедур безопасности. Настоящие Процедуры безопасности покрывают следующее:

Осы Қауіпсіздік рәсімдері Жалпы шарттармен бірге оқылуы тиіс және уақыт уақытымен қайта қарастырылуы мүмкін және Клиентке электронды байланыс құралдары арқылы немесе басқа тәсілдермен, соның ішінде, бірақ шектелмей жаңартылған Қауіпсіздік рәсімдерін CitiDirect жүйесінде жариялау арқылы жеткізіледі. Өзгесі заңнамамен көзделмеген болса, Клиентпен кез келген жоғарыда аталған қызметтерді немесе байланыс каналдарын ол Қауіпсіздік рәсімдерінің қайта қарастыруы және жаңартылуы жөнінде хабарландырылғаннан кейін қолдануы сондай қайта қарастырылған және жаңартылған Қауіпсіздік рәсімдерін қабылдау болып саналады. Осы қауіпсіздік рәсімдері мыналарды қамтиды:

A. Authentication Methods
   Способы аутентификации
   Түпнұсқаландыру әдістері
B. Customer Responsibilities
   Ответственность Клиента
   Клиенттің жауапкершілігі
C. Data Integrity and Secured Communications
   Целостность данных и защищенная связь
   Деректердің бүтіндігі және қорғалған байланыс
D. Security Manager and Related Functions
   Администратор безопасности и соответствующие функции
   Қауіпсіздік әкімшісі және сәйкес функциялар

2. Authentication Methods *Способы аутентификации* Түпнұсқаландыру әдістері

The Security Procedures include certain secure authentication methods ("Authentication Methods") which are used to uniquely identify and verify the authority of the Customer and/or any of its users authorized by the Customer typically through one or a combination of mechanisms such as user ID/password pairs, digital certificates, biometrics, security tokens (deployed via hardware or software), seal/signature verification, and/or devices associated with the Authentication Methods (collectively, the "Credentials"). Authentication Methods and associated Credentials allow the Bank to verify the origin of Communications received by the Bank.

Процедуры безопасности включают в себя определенные способы аутентификаци ("Способы аутентификации"), которые используются для достоверной идентификации и проверки полномочий Клиента и/или любого из его пользователей, уполномоченных Клиентом, как правило, с помощью таких механизмов, как: пара уникального идентификатора пользователя/пароль, цифровые сертификаты, биометрика, токены безопасности (применяемые с помощью аппаратного или программного обеспечения), проверка подлинности печати/подписи, и/или приспособления, связанные со Способами аутентификации (совместно "Данные авторизации для входа в систему"). Способы аутентификации и соответстсвующие Данные авторизации для входа в систему позволяют Банку проверить происхождение Сообщений, полученных Банком.

Қауіпсіздік рәсімдері белгілі бір түпнұсқаландыру әдістерін («Түпнұқсаландыру әдістері») қамтиды, олар әдетте пайдаланушының бірегей сәйкестендіруші жұбы/құпия сөз, санды сертификаттар, биометрика, қауіпсіздік токендері, (аппараттық немес ебағдарламалық қамтамасыз ету арқылы қолданылатын), мөрдің/қолтаңбаның дұрыстығын тексеру, және/немесе Түпнұсқаландыру әдістерімен байланысты құралдар (бірге «Жүйеге кіру үшін авторластыру деректері») сияқты механизмдері арқылы Клиенттің және/немесе оның кез келген пайдаланушысының өкілеттіктерін дұрыс түпнұсқаландыру және тексеру үшін қолданылады. Түпнұсқаландыру әдістері мен сәйкес Жүйеге кіру үшін авторластыру деректері Банкке келіп түскен хабарламалардың шыққан жерін тексеруге мүмкіндік береді.

More information regarding Authentication Methods for access to Services and/or connectivity channels may be accessed on the CitiDirect Login Help website. Customer may at any time select an available Authentication Method. During implementation of Services or connectivity channels, Bank may set-up a default Authentication Method, which Customer may change at any time to another available Authentication Method.

Более подробная информация касательно Способов аутентификации для доступа к Услугам и/или каналам связи доступна на сайте CitiDirect Login Help. Клиент может в любое время выбрать доступный Способ аутентификации. Во время применения Услуг или каналов связи Банк может установить Способ аутентификации по умолчанию, который Клиент может изменить в любое время на другой доступный Способ аутентификации.

Қызметтерге және/немесе байланыс каналдарына қолжетімділікке арналған Түпнұсқаландыру әдістері туралы толығырақ ақпарат CitiDirect Login Help сайтында бар.Клиент кез келген уақытта қолжетімді Түпнұсқаландыру әдісін таңдай алады. Қызметтер немесе байланыс каналдарын қолдану барысында Банк үнсіз келісім бойынша Түпнұсқаландыру әдісін орната алады, Клиент оны кез келген уақытта басқа қолжетімді Түпнұсқаландыру әдәсіне өзгертуге құқылы.

The following Authentication Methods are available to access the services and/or connectivity channels:

Следующие Способы аутентификации доступны для доступа к Услугам и/или каналам связи:

Қызметтерге және/немесе байланыс каналдарына қолжетімділікке арналған келесі Түпнұсқаландыру әдістері бар:

CitiDirect Authentication Methods *Способы аутентификации CitiDirect* CitiDirect Түпнұсқаландыру әдістері	
Biometrics *Биометрика* Биометрика	A digital authentication method that utilizes a user's unique physical traits, (such as a fingerprint and facial recognition), built-in biometric technology on the user's mobile device, and cryptographic techniques to gain access to CitiDirect. Physical trait data is not transferred to the Bank when the user selects this authentication method. *Цифровой способ аутентификации, который использует уникальные физические характеристики пользователя (такие как отпечаток пальца и распознование лица), биометрическую технологию, встроенную в мобильное приспособление пользователя и криптографические технические оснащения для получения доступа к CitiDirect . Данные о физических характеристиках не передаются Банку при выборе данного способа аутентификации Клиентом.* CitiDirect -ке қолжетімділікке ие болу үшін пайдаланушының бірегей физикалық сипаттамаларын (саусақтың ізі және бет-әлпетін тану), пайдаланушының ұялы құрылғысына енгізілген биометрикалық технологияны, жәнекриптографиялық техникалық жабдықтаулар арқылы іске қосылатын түпнұсқаландырудың санды әдісі. Клиент түпнұсқаландырудың осы әдісін таңдаған жағдайда физикалық сипаттамалар туралы деректер Банкке берілмейді.
Mobile Token (non-application based) *Мобильный токен без приложения* Мобильді токен (қолданбаға негізделмеген)	A digital non-application based mobile authentication method (e.g. Mobile Token (App-less)) that leverages cryptographic keys and biometric authentication (such as fingerprint and facial recognition) to link a user's mobile device to their CitiDirect account via the user's mobile browser. Physical trait data is not transferred to the Bank when the user selects this authentication method. This method facilitates multi-factor authentication by verifying the user's identity with their registered mobile device. *Цифровой метод мобильной аутентификации не требует использования приложения (мобильный токен (без приложения)). Связь мобильного устройства пользователя с его учетной записью CitiDirect осуществляется через мобильный браузер пользователя с использованием криптографических ключей и биометрической аутентификации (распознавание отпечатков пальцев и лица). Биометрические данные пользователя (физические характеристики) не передаются в Банк при выборе данного метода аутентификации. Этот метод обеспечивает многофакторную аутентификацию путем проверки личности пользователя с помощью его зарегистрированного мобильного устройства.* Пайдаланушының мобильді құрылғысын пайдаланушының мобильді браузері арқылы CitiDirect аккаунтына байланыстыру үшін криптографиялық кілттер мен биометриялық аутентификацияны (мысалы, саусақ ізі және бет-әлпетті тану) пайдаланатын қолданбаны (мысалы, Мобильді токен (қолданбасыз)) қажет етпейтін цифрлық мобильді аутентификация әдісі. Пайдаланушы осы аутентификация әдісін таңдағанда, физикалық ерекшелік туралы деректер Банкке жіберілмейді. Бұл әдіс тіркелген мобильді құрылғы арқылы пайдаланушының жеке басын растау арқылы көп факторлы аутентификацияны жеңілдетеді.

CitiDirect Authentication Methods *Способы аутентификации CitiDirect* CitiDirect Түпнұсқаландыру әдістері	
Challenge Response Token *Токен: механизм вызов-ответ* Токен: шақырту-жауап механизмі	Either (i) a mobile application based soft token (e.g. MobilePASS) or (ii) a physical token (e.g. SafeWord Card, Vasco), which in each case is used to generate a dynamic password after authenticating with a PIN (e.g. 4-digit PIN). When accessing CitiDirect, the system generates a challenge and a response passcode is generated by the utilized token and entered into the system. This authentication method, when combined with a secure password results in multifactor authentication. *Либо (i) мобильный программный токен на основе мобильного приложения (к примеру, MobilePASS) или (ii) физический токен (к примеру, SafeWord Card, Vasco), который в каждом случае используется для генерирования динамического пароля после аутентификации с помощью 4-значного пин-кода. При доступе к CitiDirect система генерирует вызов, а ответный код-пароль генерируется с помощью применимого токена и вводится в систему. Данный способ аутентификации в сочетании с безопасным паролем приводит к многофакторной аутентификации.* Немесе (i) ұялы қосымша негізіндегі ұялы бағдарламалық токен (мысалы, MobilePASS) немесе (ii) әр жағдайда 4-таңбалы пин-код арқылы түпнұсқаландырылғаннан кейін динамикалық құпиясөзді генерациялау үшін қолданылатын физикалық токен (мысалы, SafeWord Card, Vasco.). CitiDirect –ге қолжетімділік кезінде жүйе шақыртуды генерациялайды, ал жауапты құпиясөз-код қолданылатын токен арқылы генерацияланып, жүйеге енгізіледі. Түпнұсқаландырудың бұл әдісі қауіпсіз құпиясөзбен бірге қолданылатын болса, көпфакторлы түпнұсқаландыруға әкеледі.
One-Time Password Token *Токен: одноразовый пароль* Токен: бір реттік құпиясөз	Either (i) a mobile application based soft token (e.g. MobilePASS); or (ii) a physical token (e.g. SafeWord Card, Vasco) that is used to generate a dynamic password after authenticating with a PIN (e.g. 4-digit PIN). This dynamic password is entered into the system to gain access. *Либо (i) мобильный программный токен на основе мобильного приложения (к примеру, MobilePASS) или (ii) физический токен (к примеру, SafeWord Card, Vasco), который в каждом случае используется для генерирования динамического пароля после аутентификации с помощью 4-значного пин-кода. Данный динамический пароль вводится в систему для получения доступа.* Немесе (i) ұялы қосымша негізіндегі ұялы бағдарламалық токен (мысалы, MobilePASS) немесе (ii) әр жағдайда 4-таңбалы пин-код арқылы түпнұсқаландырылғаннан кейін динамикалық құпиясөзді генерациялау үшін қолданылатын физикалық токен (мысалы, SafeWord Card, Vasco.) CitiDirect -ее қолжетімділік кезінде жүйе шақыртуды генерациялайды, ал жауапты құпиясөз-код қолданылатын токен арқылы жүйеге енгізіледі.

CitiDirect Authentication Methods *Способы аутентификации CitiDirect* CitiDirect Түпнұсқаландыру әдістері	
Secure Password *Безопасный пароль* Қауіпсіз құпиясөз	A user enters his or her secure password to access the system. A secure password typically limits a user's capabilities on the system, for example, by only permitting that certain information be viewed by the user. This authentication method, when combined with a challenge response token results in multifactor authentication. *Пользователь вводит свой безопасный пароль для получения доступа в систему. Безопасный пароль, как правило, ограничивает пользовательские возможности в системе, к примеру, позволяя просмотр пользователем только определенной информации. Данный способ аутентификации в сочетании с токеном механизма вызов-ответ приводит к многофакторной аутентификации.* Жүйеге қолжетімділікке ие болу үшін пайдаланушы өзінің құпиясөзін енгізеді. Қауіпсіз құпиясөз әдетте пайдаланушының жүйедегі мүмкіндіктерін шектейді, мысалы, пайдаланушыға тек қана белгілі бір ақпаратты көруге мүмкіндік береді. ользователь вводит свой безопасный пароль для получения доступа в систему. Түпнұсқаландырудың бұл әдісі токенмен бірге қолданылатын болса, көпфакторлы түпнұсқаландыруға әкеледі.
SMS One-Time Code *Одноразовый код по SMS* SMS бойынша бір реттік код	A dynamic password delivered to users via SMS, after which the user enters the dynamic password and a secure password to gain access to the system. *Динамический пароль отправляется пользователю через SMS, после чего пользователь вводит динамический пароль и защищенный пароль для получения доступа к системе.* Динамикалық құпиясөз пайдаланушыға SMS арқылы жолданады, одан кейін пайдаланушы жүйеге қолжетімділікке ие болу үшін динамикалық құпиясөз мен қорғалған құпиясөзді енгізеді.
Voice One-Time Code *Голосовой одноразовый код* Бір реттік дауысты код	A dynamic password delivered to users via an automated voice call, after which the user enters the dynamic password and a secure password to gain access to the system. *Динамический пароль предоставляется пользователю с помощью автоматического голосового вызова, после чего пользователь вводит динамический пароль и защищенный пароль для получения доступа к системе.* Динамикалық құпиясөз пайдаланушыға автоматты түрдегі дауыстық шақырту арқылы ұсынылады, одан кейін пайдаланушы жүйеге қолжетімділікке ие болу үшін динамикалық құпиясөз мен қорғалған құпиясөзді енгізеді.

CitiDirect Authentication Methods ***Способы аутентификации CitiDirect*** **CitiDirect Түпнұсқаландыру әдістері**	
Digital Certificates *Цифровые сертификаты* Сандық сертификаттар	A digital certificate is an electronic identification issued by an approved certificate authority for authentication and authorization. Digital certificates may be attributed to corporate legal entities ("Corporate Seals") or individuals ("Personal Certificates"). The Customer is responsible for properly verifying the identity of all users of Personal Certificates acting on behalf of the Customer in accordance with local law. The Bank and the Customer are required to use digital certificates provided by authorized persons, to ensure all Communications exchanged via a public Internet connection or an otherwise unsecure Internet connection are fully encrypted and protected. *Цифровой сертификат представляет собой электронную идентификацию, выданную органом сертификации для аутентификации и авторизации. Цифровые сертификаты могут приписываться корпоративным юридическим лицам ("Корпоративная печать") либо физическим лицам ("Персональный сертификат"). Клиент несет ответственность за правильное подтверждение личностей всех пользователей Персональных сертификатов, действующих от имени Клиента в соответствии с местным законодательством.* *Банк и Клиент обязаны использовать цифровые сертификаты, предоставленные уполномоченными лицами для обеспечения полного шифрования и защиты всех Сообщений, обмен которых происходит с помощью публичного интернет соединения или иного другого небезопасного интернет соединения.* Сандық сертификат сертификаттау органымен түпнұсқаландыру және авторландыру үшін берілген электронды сәйкестендіру болып табылады. Сандық сертификаттар корпоративтік заңды тұлғаларға («Корпоративтік мөр») немесе жеке тұлғаларға («Дербес сертификат») берілуі мүмкін. Клиент жергілікті заңнамаға сәйкес Клиенттің атынан әрекет ететін Дербес сертификаттарды барлық пайдаланушылардың жеке басын дұрыс куәландыру үшін жауапты болады. Банк және Клиент олармен алмасу көпшілікті интернет байланысу немесе басқа қауіпсіз емес интернет байланысу арқылы жүзеге асырылатын барлық Хабарламаларды толық шифрлеу және қорғауын қамтамасыз ету үшін уәкілетті тұлғалармен ұсынылған сандық сертификаттарды қолдануға міндетті.

CitiConnect for Files Authentication Methods / *Способы аутентификации CitiConnect для Файлов* / Файларға арналған CitiConnect түпнұсқаландыру әдістері	
Digital Certificates *Цифровые сертификаты* Сандық сертификаттар	See description above. *Смотреть описание выше.* Жоғарыдағы сипаттаманы қараңыз.

CitiConnect for Files Authentication Methods / *Способы аутентификации CitiConnect для Файлов* / Файларға арналған CitiConnect түпнұсқаландыру әдістері	
IP Address Whitelist When Using CitiConnect *Занесение IP-адреса в белый список при CitiConnect* CitiConnect жағдайында IP-мекенжайды ақ тізімге енгізу	Certain Internet communications received by the Bank, for example, via a Virtual Private Network (VPN), may also rely on the parties exchanging information using pre-agreed Internet Protocol (IP) addresses. The Bank will only accept communications originating from the Customer's designated IP address, and vice versa; and the Bank will only transmit Communications to the Customer's designated IP address, and vice versa. Used in conjunction with Digital Certificate method above. *Некоторые сообщения, полученные Банком с помощью интернета, к примеру, по средствам Virtual Private Network (VPN), могут также передоваться сторонами используя заранее согласованный IP-адрес. Банк будет принимать только сообщения, исходящие из указанного IP-адреса Клиента, и наоборот, а также Банк будет направлять сообщения только на указанный IP-адрес Клиента, и наоборот. Данный способ используется совместно с Цифровым сертификатом, указанным выше.* Банкке интернет арқылы, мысалы Virtual Private Network (VPN) арқылы келіп түскен кейбір хабарламалар сондай-ақ тараптармен алдын ала келісілген IP-мекенжайды қолдана отырып жолданылуы мүмкін. Банк Клиенттің аталған IP-менжайынан келген хабарламаларды ғана қабылдайтын болады, санымен қатар, Банк хабарламаларды Клиенттің аталған IP-мекенжайына ғана жолдайтын болады, және керісінше. Бұл әдіс жоғарыда аталған Сандық сертификатпен бірге қолданылады.

CitiConnect API Authentication Methods / *Способ аутентификации CitiConnect API* / CitiConnect API түпнұсқаландыру әдісі	
Digital Certificates *Цифровые сертификаты* Сандық сертификаттар	See description above. *Смотреть описание выше.* Жоғарыдағы сипаттаманы қараңыз.
IP Address Whitelist When Using CitiConnect *Занесение IP-адреса в белый список при CitiConnect* CitiConnect жағдайында IP-мекенжайды ақ тізімге енгізу	See description above. *Смотреть описание выше.* Жоғарыдағы сипаттаманы қараңыз.

CitiConnect for SWIFT Authentication Methods / *Способ аутентификации CitiConnect для SWIFT* / SWIFT-ке арналған CitiConnect түпнұсқаландыру әдісі	
Digital Certificates *Цифровые сертификаты* Сандық сертификаттар	See description above. Can be used in conjunction with SWIFT Authentication method below. *Смотреть описание выше. Данный способ может использоваться совместно со способом Аутентификация через SWIFT, указанным ниже.* Жоғарыдағы сипаттаманы қараңыз. Бұл әдіс төменде көрсетілген SWIFT арқылы Түпнұсқаландыру әдісімен бірге қолданылуы мүмкін.

CitiConnect for SWIFT Authentication Methods / *Способ аутентификации CitiConnect для SWIFT* / SWIFT-ке арналған CitiConnect түпнұсқаландыру әдісі	
SWIFT Authentication *Аутентификация через SWIFT* SWIFT арқылы Түпнұсқаландыру	Communications sent between the Bank and the Customer via the SWIFT network, including, but not limited to, account information, payment orders, and instructions to amend or cancel such orders, will be authenticated using procedures defined in SWIFT's Contractual Documentation (as amended or supplemented from time to time) which includes without limitation its General Terms and Conditions and FIN Service Description or as set forth in other terms and conditions that may be established by SWIFT. The Bank is not obliged to do anything other than what is contained in the SWIFT procedures to establish the sender and authenticity of these Communications. The Bank is not responsible for any errors or delays in the SWIFT system. The Customer is responsible for providing communications to the Bank in the format and type required and specified by SWIFT. Transmissions and Communications sent or received via SWIFT facilities are subject to SWIFT rules and regulations in effect, including membership rules. The Customer is responsible for being familiar with and conforming to SWIFT messaging standards. *Сообщения, отправляемые между Банком и Клиентом через сеть SWIFT, включая, но не ограничиваясь, информацией о счете, платежных поручениях и инструкции по изменению или отмене таких поручений, будут аутентифицированы используя процедуры, определенные в Договоре на обслуживание SWIFT (с учетом изменений и дополнений, вносимых время от времени), который включает без ограничения Общие положения и описание услуги FIN или как предусмотрено в любых других условиях, которые могут быть установлены SWIFT. Банк не обязан предпринимать какие-либо действия кроме тех, которые содержатся в процедурах SWIFT для установления отправителя и подлинности Сообщений.* *Банк не несет ответственности за какие-либо ошибки или задержки в системе SWIFT. Клиент несет ответственность за предоставление Банку сообщений в таком формате и в таком виде, которые требуются и определены SWIFT.* *Передача данных и Сообщений, отправленных либо полученных с помощью сооружений и оборудования SWIFT подпадают под действие действующих правил и инструкций SWIFT, включая правила членства. Клиент несет ответственность за ознакомление и соответствие стандартам передачи сообщений SWIFT.* SWIFT арқылы Банк пен Клиент арасында жолданатын хабарламалар, соның ішінде, бірақ шектелмей, шот туралы ақпарат, төлем тапсырмалар мен сондай тапсырмаларды өзгерту немесе күшін жою туралы ақпарат SWIFT қызмет көрсету Шартында (уақыт уақытымен енгізілетін өзгертулер мен толықтыруларды ескере отырып) белгіленген рәсімдерді қолдана отырып түпнұсқаландырылатын болады, аталған Шарт шектеусіз Жалпы ережелерді және FIN қызметтерінің сипаттамасын немесе SWIFT-пен орнатылатын кез келген басқа шарттарда көзделгендерді қамтиды. Банк Хабарламаларды жолдаушыны және оның түпнұсқалығын тексеру үшін SWIFT рәсімдерінде көрсетілгеннен басқа қандай да басқа шаралар қолдануға міндетті емес. Банк SWIFT жүйесінде орын алған қандай да қателер немесе кешіктірулер үшін жауапты емес. Клиент Банкке хабарламлар ұсыну үшін SWIFT-пен талап етілген және белгіленген нысанда және түрде жауапкершілікке тартылады. SWIFT құрылғылары мен жабдықтары арқылы жолданған немесе қабылданған Хабарламаларды жөнелту мүшелік туралы ережелерді қоса алғанда, SWIFT әрекетті ережелер мен нұсқаулықтар бойынша жүзеге асыралады. Клиент SWIFT хабарламларды жөнелту стандарттарымен танысу және сәйкестігі үшін жауапты болады.

SWIFT Authentication Method / ***Способо аутентификации SWIFT*** / **SWIFT түпнұсқаландыру әдісі**	
SWIFT Authentication (Direct Connection for Financial Institutions) *Аутентификация через SWIFT (Прямое соединение для финасовых институтов)* SWIFT арқылы түпнұсқаландыру (Қаржы институттарына арналған тікелей қосу)	Communications sent between the Bank and the Customer via the SWIFT network, including, but not limited to, account information, payment orders, and instructions to amend or cancel such orders, will be authenticated using procedures defined in SWIFT's Contractual Documentation (as amended or supplemented from time to time) which includes without limitation its General Terms and Conditions and FIN Service Description or as set forth in other terms and conditions that may be established by SWIFT. The Bank is not obliged to do anything other than what is contained in the SWIFT procedures to establish the sender and authenticity of these Communications. The Bank is not responsible for any errors or delays in the SWIFT system. The Customer is responsible for providing communications to the Bank in the format and type required and specified by SWIFT. Transmissions and Communications sent or received via SWIFT facilities are subject to SWIFT rules and regulations in effect, including membership rules. The Customer is responsible for being familiar with and conforming to SWIFT messaging standards. *Сообщения, отправляемые между Банком и Клиентом через сеть SWIFT, включая, но не ограничиваясь, информацией о счете, платежных поручениях и инструкции по изменению или отмене таких поручений, будут аутентифицированы используя процедуры, определенные в Договоре на обслуживание SWIFT (с учетом изменений и дополнений, вносимых время от времени), который включает без ограничения Общие положения и описание услуги FIN или как предусмотрено в любых других условиях, которые могут быть установлены SWIFT. Банк не обязан предпринимать какие-либо действия кроме тех, которые содержатся в процедурах SWIFT для установления отправителя и подлинности Сообщений.* *Банк не несет ответственности за какие-либо ошибки или задержки в системе SWIFT. Клиент несет ответственность за предоставление Банку сообщений в таком формате и в таком виде, которые требуются и определены SWIFT.* *Передача данных и Сообщений, отправленных либо полученных с помощью сооружений и оборудования SWIFT подпадают под действие действующих правил и инструкций SWIFT, включая правила членства. Клиент несет ответственность за ознакомление и соответствие стандартам передачи сообщений SWIFT.* SWIFT арқылы Банк пен Клиент арасында жолданатын хабарламалар, соның ішінде, бірақ шектелмей, шот туралы ақпарат, төлем тапсырмалар мен сондай тапсырмаларды өзгерту немесе күшін жою туралы ақпарат SWIFT қызмет көрсету Шартында (уақыт уақытымен енгізілетін өзгертулер мен толықтыруларды ескере отырып) белгіленген рәсімдерді қолдана отырып түпнұсқаландырылатын болады, аталған Шарт шектеусіз Жалпы ережелерді және FIN қызметтерінің сипаттамасын немесе SWIFT-пен орнатылатын кез келген басқа шарттарда көзделгендерді қамтиды. Банк Хабарламаларды жолдаушыны және оның түпнұсқалығын тексеру үшін SWIFT рәсімдерінде көрсетілгеннен басқа қандай да басқа шаралар қолдануға міндетті емес. Банк SWIFT жүйесінде орын алған қандай да қателер немесе кешіктірулер үшін жауапты емес. Клиент Банкке хабарламлар ұсыну үшін SWIFT-пен талап етілген және белгіленген нысанда және түрде жауапкершілікке тартылады. SWIFT құрылғылары мен жабдықтары арқылы жолданған немесе қабылданған Хабарламаларды жөнелту мүшелік туралы ережелерді қоса қанда, SWIFT әрекетті ережелер мен нұсқаулықтар бойынша жүзеге асыралады. Клиент SWIFT хабарламларды жөнелту стандарттарымен танысу және сәйкестігі үшін жауапты болады.

Digital/Electronic Signature Authentication Methods for Electronic Document Submission *Способ аутентификации для подачи электронного документа Цифровая/Электронная Подпись* Сандық/Электронды Қолтаңба электронды құжатын ұсынуға арналған түпнұсқаландыру әдісі	
Digital Signature *Цифровая подпись* Сандық қолтаңба	A type of electronic signature that leverages digital certificates to validate the authenticity and integrity of a signature, message, software or digital document. *Вид электронной подписи, применяющий цифровые сертификаты для подтверждения подлинности и целостности подписи, сообщения, программного обеспечения или цифрового документа.* Қолтаңбаның, хабарламаның, бағдарламалық қамтамасыз етудің және сандық құжаттың дұрыстығы мен бүтіндігін растауға арналған сандық сертификаттарды қолданатын электронды қолтаңбаның түрі.
Electronic Signature *Электронная подпись* Электронды қолтаңба	An electronic symbol attached to a contract or other record, unique to and used by a person with an intent to sign. Electronic signatures can be established in the form of words, letters, numerals, symbols, click of a button on a website, upload of facsimile or scan of a physical signature, signing on a touchscreen, or agreeing to any terms and conditions by electronic means. Created under the sole control of the person using it, it is logically attached to or associated with a data message, capable of identifying the person who consents to the data message and certifying the person's consent. Such Electronic Signature would be submitted to the Bank through the Bank's electronic channels and in compliance with the associated Authentication Methods described above. *Электронный символ, прилагаемый к договору или иной записи, присущий лицу и используемый им с целью подписания. Электронные подписи могут быть установлены в форме слов, букв, цифр, символов, щелчка кнопки на интернет-сайте, загрузки факсимиле или сканированной копии физической подписи, подписи на сенсорном дисплее либо соглашения электронным способом с положениями и условиями. Созданная для единоличного контроля лицом, использующим цифровую подпись, цифровая подпись логически прилагается к или связана с сообщением данных, способных идентифицировать лицо, соглашающееся с сообщением данных и подтверждающее согласие лица. Данная Электронная подпись будет подана Банку через электронные каналы Банка и отвечает соответствующим Способам аутентификации, указанным выше.* Тұлғаға тиесілі немесе ол қол қою үшін қолданылатын, шартқа немесе басқа жазбаға қоса берілетін электронды таңба. Электронды қолтаңбалар сөздер, әріптер, сандар нысанында, интернет сайтта батырманы шерту, факсимиле жүктеу немесе жеке тұлғаның қолын, сенсорлы дисплейдегі қолтаңбаны сканерлеу арқылы немесе ережелермен немесе талаптармен электронды нысанда келісу арқылы орнатылуы мүмкін. Сандық қолтаңбаны қолданылатын тұлғамен дербес бақылау үшін құрылған сандық қолтаңба деректерді хабарлап отырған және тұлғаның келісуін растайтын хабарламамен келісетін тұлғаны сәйкестендіруге қабілетті деректерге қоса беріледі немесе онымен байланысты болып табылады. Бұл Электронды қолтаңба Банкке Банк каналдары арқылы ұсынылатын болады және жоғарыда көрсетілген Түпнұсқаландырудың әдістеріне сәйкес келеді.

Manual Initiated Funds Transfer (MIFT) Authentication Method *Способ аутентификации Платежная инструкция на бумажном носителе (MIFT)* Қағаз тасымалдауыштағы төлем нұқсамасы Түпнұсқаландыру әдісі (MIFT)	
MIFT Authentication *Аутентификация через MIFT* MIFT Түпнұсқаландыру	Manually Initiated Funds Transfer (MIFT), including amendments, recalls, or cancelations of previous manual instructions, may be made by fax or letter or upload to CitiDirect. Not all forms are supported in all countries. Initiators are persons designated by the Customer who are authorized to initiate transactions in accordance with restrictions, if any, are identified by the Customer. Confirmers are person designated by the Customer that Bank may call back, at its discretion, for confirmation of manually initiated instructions for funds transfers. In certain countries, mobile telephone numbers are not accepted as call back numbers. Further details are provided in the applicable Country Cash Management User Guide, Global Manual Transaction Authorization or Universal Nomination Form. MIFT is to be used by the Customer as a contingency method to communicating instructions to the Bank. *Платежная инструкция на бумажном носителе (MIFT), включая изменения, отзывы или отмены предыдущих платежных инструкций, может быть осуществлена факсом или письмом или загрузкой на CitiDirect. Не все формы поддерживаются во всех странах. Инициаторами являются лица, назначенные Клиентом и уполномоченные на инициирование сделок в соответствии с ограничениями, установленными Клиентом, если таковые имеются. Подтверждающими лицами являются лица, назначенные Клиентом, которым Банк по собственному усмотрению может перезвонить для подтверждения платежных инструкций на бумажном носителе.* *В некоторых странах мобильные телефонные номера не воспринимаются как номера обратного вызова. Дополнительные сведения предоставлены в соответствующем Пользовательском руководстве по странам по управления наличными средствами, Глобальной авторизации платежной транзакции или Форме универсального номинирования. MIFT подлежит использованию Клиентом в качестве чрезвычайного метода передачи инструкций Банку.* Қағаз тасымалдаушыдағы төлем нұсқамулық (MIFT), соның ішінде алдыңғы төлем нұсқаулықтарды өзгерту, кері қайтару немесе күшін жоюлар факс немесе хат арқылы немесе CitiDirect –ге жүктеу арқылы жүзеге асырылады. Нысандардың кейбіреуі барлық елдерде қолданылмайды. Бастамашы ретінде Клиентпен орнатылған, бар болған жағдайда, шектеулерге сәйкес Клиентпен мәмілелерді бастама етуге тағайындалған және уәкілдірілген тұлғалар болып табылады. Растаушы тұлғалар ретінде оларға Банк өзінің қарауы бойынша қағаз тасымалдауыштағы төлем нұсқаулықтарды растау үшін қайта қоңырау шала алатын Клиентпен тағайындалған тұлғалар болып табылады. Кейбір елдерде ұсялы телефондар кері байланысқа арналған нөмірлер ретінде қарастырылады. Қосымша мәліметтер елдер бойынша қолма-қол ақшаны басқару, Төлем транзакциясын ғаламдық авторландыру немесе әр жақты номинациялау нысаны бойынша сәйкес Пайдалану жөніндегі басшылықта ұсынылған. Дополнительные. MIFT Банкке нұсқаулықтар табыстаудың төтенше әдісі ретінде Клиентпен қолдануына жатады.

Mail, Fax, Email and Messenger Authentication Methods *Способ аутентификации Письмо, Факс, Электронная почта и Мессенджер* Хат, Факс, Электронды пошта және Мессенджер түпнұсқаландыру әдісі	
Seal Image Verification *Подтверждение изображения печати* Мөрдің бейнесін растау	Correspondence received by the Bank via fax, mail, email or messenger, excluding MIFT requests, are verified and collated with due care based on the seal image contained in the Customer's authority document or similar document provided to the Bank. *Корреспонденция, полученная Банком с помощью факса, почты, электронной почты или мессенджера, за исключением запросов MIFT, с надлежащей осмотрительностью подтверждается и сверяется на основе изображения печати, содержащегося в документе о полномочиях Клиента или похожем документе, предоставленном Банку.* Банк MIFT сұраныстарын қоспағанда, факс, пошта, электронды пошта немесе мессенджер арқылы алған хат-хабар тиісті абайлықпен расталып, Клиенттің өкілеттіктері туралы құжатта немесе Банкке ұсынылған ұқсас құжатта көрсетілген мөрдің бейнесімен салыстырылады.
Signature Verification *Подтверждение подписи* Қолтаңбаны растау	Correspondence received by the Bank via fax, mail, email or messenger, excluding MIFT requests, are signature verified based on the information contained in the Customer's authority document or similar document provided to the Bank. *Корреспонденция, полученная Банком с помощью факса, почты, электронной почты или мессенджера, за исключением запросов MIFT, подтверждается подписью на основе информации, содержащейся в документе о полномочиях Клиента или похожем документе, предоставленном Банку.* Банк MIFT сұраныстарын қоспағанда, факс, пошта, электронды пошта немесе мессенджер арқылы алған хат-хабар Клиенттің өкілеттіктері туралы құжатта немесе Банкке ұсынылған ұқсас құжатта қамтылған ақпарат негізінде қолтаңбамен расталады.
Secure PDF *Защищенный паролем файл PDF* Құпиясөзбен қорғалған PDF файлы	Encrypted emails are delivered to a regular mailbox as PDF documents that are opened by entering a private password. Both the message body and any attached files are encrypted. A private password can be set up upon receipt of the first secure email received. *Зашифрованные электронные письма доставляются в обычный почтовый ящик в виде документа в формате PDF, который открывается с помощью личного пароля. Само сообщение, и все прикрепленные файлы зашифровываются. Личный пароль можно настроить после получения первого сообщения по защищенной электронной почте.* Шифрленген электронды хаттар жеке құпиясөз арқылы ашылатын PDF нысанындағы құжат түрінде кәдімгі пошта жәшігіне жеткізіледі. Хабарламаның өзі және барлық қоса берілген файлдар шифрленеді. Жеке құпиясөзді қорғалған электронды пошта арқылы бірінші хабарламаны алғанннан кейін баптауға болады.

Mail, Fax, Email and Messenger Authentication Methods *Способ аутентификации Письмо, Факс, Электронная почта и Мессенджер* Хат, Факс, Электронды пошта және Мессенджер түпнұсқаландыру әдісі	
MTLS *MTLS* MTLS	Mandatory Transport Layer Security (MTLS) creates what would be a secure, private email connection between the Bank and the Customer. Emails transmitted using this channel are sent over the Internet through an encrypted TLS tunnel created by the connection. *Протокол Mandatory Transport Layer Security (MTLS) (Протокол защиты транспортного уровня) создает безопасное частное соединение по электронной почте между Банком и Клиентом. Электронные письма, отправленные с использованием этого канала, отправляютсяс помощью интернета через зашифрованный канал TLS, созданный соединением.* Mandatory Transport Layer Security (MTLS) хаттамасы (Көлік деңгейіндегі қорғау хаттамасы) Банк пен Клиент арасында электронды пошта арқылы қауіпсіз меншік байланысты орнатады. Бұл каналды қолдана отырып жолданған электронды хаттар байланыспен орнатылған шифрленген TLS канал арқылы интернет бойынша жолданады.

Phone Authentication Methods / *Способ аутентификации Телефон* / Телефон түпнұсқаландыру әдісі	
PIN *PIN код* PIN код	Customers contacting the Bank via phone are prompted to enter a PIN to validate authorized access. *Клиенты, связывающиеся с Банком с помощью телефона должны ввести PIN-код чтобы подтвердить авторизованный доступ.* Банкпен телефон арқылы байланысып отырған клиенттер авторландырылған қолжетімділікті растау үшін PIN-код енгізуге тиіс.
Verification Questions *Подтверждающие вопросы* Растау сұрақтары	Customers contacting the Bank via phone are prompted by the Bank's service representatives to provide correct verbal responses to verification questions in order to validate authorized access. *Клиенты, связывающиеся с Банком с помощью телефона должны предоставить представителям Банка вербальные ответы на подтверждающие вопросы чтобы подтвердить авторизованный доступ.* Банкпен телефон арқылы байланысып отырған клиенттер авторландырылған қолжетімділікті растау үшін Банктің өкілдеріне растау сұрақтарына ауызша жауаптар ұсынуы тиіс. Клиенты, связывающиеся с Банком с помощью телефона должны предоставить представителям Банка вербальные ответы на подтверждающие вопросы чтобы подтвердить авторизованный доступ.

The availability of Authentication Methods described above varies based on local markets.

Доступность Способов аутентификации, описанная выше варьируется в зависимости от местных рынков.

Жоғарыда сипатталған Түпнұсқаландыру әдістерінің қолжетімділігі жергілікті нарықтарға байланысты өзгеруі мүмкін.

3. Customer Responsibilities
Ответственность Клиента
Клиенттің жауапкершілігі

3.1 Identifying Authorized Users: Customer is responsible for identifying: (i) all individuals acting on the Account(s) on behalf of the Customer at an entity level for all Services and connectivity channels, and (ii) each person acting on behalf of the Customer being duly authorized by the Customer to act on the Customer's Account.

Определить уполномоченных пользователей: Клиент несет ответственность за определение: (i) всех физических лиц, действующих по Счету(-ам) от имени Клиента на уровне организации в отношении всех Услуг и каналов связи, и (ii) каждое лицо, действующее от имени Клиента надлежащим образом уполномоченно Клиентом действовать по Счету Клиента.

Уәкілетті пайдаланушыларды айқындау: Клиент (i) барлық Қызметтер және байланыс каналдарына қатысты ұйым деңгейінде Клиенттің атынан Шот(тар) бойынша әрекет ететін барлық жеке тұлғаларды, және (ii) Клиенттің атынан әрекет ететін әрбір тұлға Клиентпен Клиенттің Шоты бойынша әрекет етуге тиісті түрде уәкілдірілгенін айқындау үшін жауапты болады.

3.2 Customer is responsible for assigning and monitoring any transaction limits assigned to the Customer and/or its users and ensuring that these limits (a) do not exceed the limits as required by the Customer's internal policies and other authority and constitutive documents such as Customer's Board of Director resolutions, Bank Mandates, Power Of Attorney, or equivalent document, and (b) are properly reflected on all connectivity channels and user entitlements.

Клиент несет ответственность за установление и мониторинг любых транзакционных лимитов установленных Клиенту и/или его пользователям и обеспечивает то, что эти лимиты (a) не будут превышать лимиты, установленные внутренними политиками Клиента и другими документами о полномочиях и учредительными документами, такими как решения Совета директоров Клиента, Мандат Банка, Доверенности либо равноценным документом, и (b) правильно отражены во всех каналах связи и документах, касающихся прав пользователей.

Клиент Клиентке және/немесе оның пайдаланушыларына орнатылған кез келген транзакциялық лимиттерді орнату үшін жауапты болады және аталған лимиттер (a) Клиенттің ішкі саясаттарымен және өкілеттіктер туралы басқа құжаттармен және Клиенттің Директорлары кеңесінің, Банк Мандаты, Сенімхаттар немесе ұқсас құжаттар сияқты құрылтай құжаттарымен белгіленген лимиттерден аспайтынын, және (b) барлық каналдар мен пайдаланушының құқықтарына қатысты құжаттарда дұрыс көрсетілуін қамтамасыз етеді.

3.3 Certain jurisdictions may require individuals (and their corresponding Credentials) to be identified by the Bank in accordance with applicable AML legislation requirements before granting access to perform certain functions. Please contact your Customer Service Representative or visit the CitiDirect website for further information.

Некоторые юрисдикции могут потребовать Банк идентифицировать физических лиц (и их соответствущие Данные авторизации для входа в систему) до предоставления Банком доступа к выполнению некоторых функций в соответствии с применимыми требованиями законодательства о противодействии отмыванию денег. Пожалуйста, свяжитесь с Вашим Представителем Службы поддержки либо посетите интернет-страницу CitiDirect для дополнительной информации.

Кейбір юрисдикциялар Банктен ақшаны жылыстауға қарсылық білдіру туралы қолданыстағы заңнаманың талаптарына сәйкес Банкпен кейбір функцияларды орындауға қолжетімділікті ұсынғанға дейін жеке тұлғаларды сәйкестендіруін (және олардың тиісті Жүйеге кіру үшін авторластыру деректерін) талап етуі мүмкін. Қосымша ақпарат қажет болған жағдайда Сіздің Қолдау қызметіңіздің өкілімен байланысуыңызды немесе CitiDirect интернет-парақшасына кіруіңізді өтінеміз.

3.4 Safeguarding of Authentication Methods
Сохранность Способов аутентификации
Түпнұсқаландыру әдістерінің сақталуы

The Customer is responsible for safeguarding the Authentication Methods and Credentials with the highest standard of care and diligence, and ensuring that access to and distribution of the Credentials are limited only to persons that have been authorized by the Customer.

Communications sent by a third party: Where the Customer is using a Credential to identify and authenticate their Communications as originating from them as a legal entity, the Customer is responsible for exercising full control over the use of such Credentials when sending Communications to the Bank, including where such Communications are sent by applications and/or systems that are managed by a third party on behalf of the Customer. In all circumstances the Bank will (a) deem any Communication it receives through an electronic connectivity channel, that has been received by the Bank in compliance with these Security Procedures duly authenticated as originating from the Customer, as a Communication instructed by the Customer and (b) may act upon any Communication that it receives on behalf of the Customer in compliance with these Security Procedures.

Клиент несет ответственность за сохранность Способов аутентификации и Данных авторизации для входа в систему с высокой степенью заботливости и осмотрительности и гарантирует то, что доступ к Данным авторизации для входа в систему и их распространение будут ограничены только кругом лиц, уполномоченных Клиентом.

Сообщения отправляемые третьей стороной: Там, где Клиент использует Данные авторизации для входа в систему для идентификации и аутентификации своих Сообщений, происходящих от него как юридического лица, Клиент несет ответственность за полный контроль над использованием таких Данных авторизации для входа в систему при отправлении Сообщений Банку, включая ситуации, в которых Сообщения отправляются путем заявки и/или системами, которые управляются третьей стороной от имени Клиента. Во всех случаях Банк (a) будет презюмировать, что любые Сообщения, полученные им посредством электронных каналов связи в соответствии с данными Процедурами безопасности и должным образом аутентифицированными как происходящими от Клиента, являются Сообщениями, порученными Клиентом и (b) может действовать на основании любого Сообщения, полученного им от имени Клиента в соответствии с настоящими Процедурами безопасности.

Клиент жоғары деңгейдегі қамқорлықпен және абайлықпен Түпнұсқаландыру әдістері мен Жүйеге кіру үшін авторластыру деректерінің сақталуы үшін жауапты болады және Жүйеге кіру үшін авторластыру деректеріне қолжетімділік және оларды тарату құқығы Клиентпен уәкілдірілген тұлғалармен ғана шектелетініне кепілдік береді.

Үшінші тараптармен жолданылатын хабарламалар: Клиент өзінен заңды тұлға ретінде жолданылатын өзінің Хабарламаларының түпнұсқаландыру және сәйкестендіру үшін Жүйеге кіру үшін авторластыру деректерін қолданылатын жерлерде Клиент Хабарламалар Клиенттің атынан үшінші тұлғалармен басқарылатын тапсырыс беру және/немесе жүйелермен жолданылатын жағдайларды қоса, Банкке Сәйкестендіру Хабарламаларды жолдау кезінде сондай Жүйеге кіру үшін авторластыру деректерді қолдануын толығымен бақылауы үшін жауапты болады. Барлық жағдайларда Банк (a) өзі осы Қауіпсіздік рәсімдеріне сәйкес электронды байланыс каналдары арқылы алған және Клиенттен келіп түскен ретінде тиісті түрде түпнұсқаландырылған кез келген Хабарламалар Клиентпен алынған Хабарламалар болып табылатынын презумциялайтын болады, және (b) өзі Клиенттің атынан осы Қауіпсіздік рәсімдеріне сәйкес алған кез келген Хабарлама негізінде әрекет ете алады.

4. Data Integrity and Secured Communications *Целостность данных и защищенная связь* Деректердің бүтіндігі және қорғалған байланыс

4.1 The Customer will be transmitting data to and otherwise exchanging Communications with the Bank, utilizing the internet, mail, email and/or fax which the Customer understands are not (i) necessarily secure communications and delivery systems, and (ii) under the Bank's control. The Customer further understands that if Customer's users are entitled to access Open Banking and/or similar third-party platforms outside of the Citi systems, Customer data could be transmitted over such third-party platforms which are not under the Bank's control.

Клиент будет передавать данные в Банк и иным образом обмениваться сообщениями с ним, используя Интернет, почту, в частности электронную почту, и/или факс, которые, по мнению Клиента, (i) не являются гарантированно безопасными системами связи и доставки, (ii) не находятся под контролем Банка. Клиент также осознает, что если пользователи Клиента имеют право доступа к Открытому банкингу и/или подобным сторонним платформам вне систем Citi, данные Клиента могут передаваться через такие сторонние платформы, которые не находятся под контролем Банка.

Клиент Банкпен интернет, пошта, электрондық пошта және/немесе факс арқылы деректерді беріп, хабар алмасады. Бұл ретте Клиент келесілерді түсінеді: (i) бұл байланыс және жеткізу жүйелері міндетті түрде қауіпсіз болмауы мүмкін және (ii) олар Банктің бақылауында болмайды. Клиент сонымен қатар егер Клиенттің пайдаланушылары Citi жүйелерінен тыс Open Banking және/немесе осыған ұқсас үшінші тарап платформаларына кіруге рұқсаты болса, Клиенттің деректері Банктің бақылауында емес осындай үшінші тарап платформалары арқылы берілуі мүмкін екенін түсінеді.

4.2 The Bank, utilizes industry leading encryption methods (as determined by the Bank), which help to ensure that information is kept confidential and that it is not changed during electronic transit.

Банк использует передовые, принятые в отрасли, методы шифрования (определяемых самостоятельно Банком), которые помогают обеспечить конфиденциальность информации и невозможность изменения данных во время их передачи.

Банк ақпараттың құпиялылығын және оларды табыстау барысында деректердің өзгермейтіндігін қамтамасыз етуге мүмкіндік беретін алдағы, салада қолданылатын шифрлеу әдістерін (Банкпен жеке белгіленетін) қолданады.

4.3 If the Customer suspects or becomes aware of a technical failure or any improper or potentially fraudulent access to or use of the Bank's Services or connectivity channels or Authentication Methods by any person (whether an authorized person or not), the Customer shall promptly notify the Bank of such occurrence. In the event of improper or potentially fraudulent access or use by an authorized person, the Customer should take immediate actions to terminate such authorized person's access to and use of the Bank's Services or connectivity channels.

Если Клиент подозревает или ему становится известно о техническом сбое или несанкционированном доступе, или ненадлежащем использовании Услуг Банка, каналов подключения или Способов аутентификации любым лицом (независимо от того, является ли оно уполномоченным лицом или нет), Клиент должен незамедлительно уведомить Банк об этом. В случае, если уполномоченное лицо Клиента получило ненадлежащим образом доступ или воспользовалось услугами или каналами связи, то Клиент должен незамедлительно принять меры для прекращения доступа такого уполномоченного лица к Услугам и каналам связи Банка и их использованию.

Егер Клиент Банктің қызметтерін, қосу арналарын немесе түпнұсқаландыру әдістерін кез-келген тұлға (ол уәкілетті тұлға екеніне немесе уәкілетті тұлға еместігіне қарамастан) тиісті түрде пайдаланбағаны немесе рұқсат етілмеген қолжетімдігі немесе техникалық кідірісі туралы күдіктенсе немесе оған мәлім болса, онда Клиент бұл туралы Банкке дереу хабарлауы тиіс.Егер,

Клиенттің уәкілетті тұлғасы қызметтерге немесе байланыс арналарына қолжетімдікті немесе пайдалануды тиісті емес түрде іске қолданған жағдайда осындай тұлғаның Банктің қызметтеріне және байланыс арналарына қолжетімдігін және пайдалануын тоқтату үшін Клиент дереу тиісті шараларды қабылдауы тиіс.

4.4 If the Customer utilizes file formatting or encryption software (whether provided by the Bank or a third party) to support the formatting and recognition of the Customer's data and instructions and acts upon Communications with the Bank, the Customer will use such software solely for the purpose for which it has been installed.

Если Клиент использует программное обеспечение для форматирования файлов или шифрования (независимо от того, предоставлено ли оно Банком или третьим лицом) для поддержки форматирования и распознавания данных и инструкций Клиента и действует в отношении Сообщений с Банком, то Клиент будет использовать такое программное обеспечение исключительно для тех целей, для которых оно было установлено.

Егер Клиенттің деректері мен нұсқаулықтарын форматтау және айырып тануды қолдау үшін Клиент файлдарды форматтауға және шифрлеуге арналған бағдарламалық қамтамасыздандыруды (оны Банк немесе үшінші тұлға ұсынғанына қарамастан) пайдаланса және Банкпен арадағы хабарламаларға қатысты әрекет етсе, онда Клиент осындай бағдарламалық қамтамасыздандыруды ол белгіленген мақсаттары үшін ғана пайдаланатын болады.

4.5 The Customer accepts that the Bank may suspend or deny users' access to Services requiring the use of Credentials (i) in case of suspicion of unauthorized or fraudulent use of the Credentials and/or (ii) to safeguard the Services or Credentials.

Клиент соглашается с тем, что Банк может приостановить доступ пользователей к Услугам, которые требуют использования Данных авторизации для входа в систему для получения доступа к системе (i) в случае подозрения в несанкционированном или мошенническом использовании Данных авторизации для входа в систему и/или (ii) для того, чтобы защитить Услуги или Данные авторизации для входа в систему.

(i) Жүйеге кіру үшін авторластыру деректерін рұқсат етілмеген пайдалануға немесе алаяқтыққа қатысты күдік туындаған жағдайда және/немесе (ii) Қызметтерді және/немесе Жүйеге кіру үшін авторластыру деректерін қорғау үшін жүйеге қолжетімдік алу үшін Жүйеге кіру үшін авторластыру деректерін пайдалануды талап ететін Қызметтерге Пайдаланушылардың қолжетімдігін Банк уақытша тоқтата алады дегенмен Клиент келіседі.

5. Security Manager and Related Functions
Администратор безопасности и соответствующие функции
Қауіпсіздік әкімшісі және сәйкес функциялар

For applications accessible in CitiDirect and CitiConnect (with the exception of Personal Certificates discussed below), the Bank requires the Customer to establish a "Security Manager" function. Security Managers are responsible for:

Для приложений, доступных в CitiDirect и CitiConnect (за исключением Персональных сертификатов, упомянутых ниже), Банк требует, чтобы Клиент назначил функцию «Менеджера по безопасности». Менеджеры по безопасности несут ответственность за:

CitiDirect және CitiConnect-те қолжетімді қолданбалар үшін (төменде айтылатын жеке куәліктерден басқа) Банк Клиенттен "Қауіпсіздік менеджері" функциясын орнатуды талап етеді. Қауіпсіздік менеджерлері мыналар үшін жауапты:

5.1 Establishing and maintaining the access and entitlements of users (including Security Managers themselves) including activities such as: (a) creating, deleting or modifying user Profiles (including Security Manager Profiles) and entitlement rights (Note that user name must align with supporting identification documents); (b) building access profiles that define the functions and data available to individual users; (c) enabling and disabling user log-on credentials; and (d) assigning transaction limits (Note these limits are not monitored or validated by the Bank and Customer should monitor these limits to ensure they are in compliance with the Customer's internal policies and requirements, including but not limited to, those established by the Customer's Board of Directors or equivalent);

Предоставление и текущая поддержка доступа и прав пользователей (включая самих Администраторов безопасности), в том числе следующие функции как: (a) создание, удаление или изменение Профилей пользователя (в том числе Профилей Администраторов безопасности) и наделение полномочиями (обратите внимание, что имя пользователя должно совпадать с удостоверяющими документами); (b) создание профилей доступа, которые определяют функции и данные, доступные индивидуальным пользователям; (c) подключение и отключение учетных данных входа; и (d) определение транзакционных лимитов (обратите внимание, что данные лимиты не контролируются или утверждаются Банком и Клиент должен контролировать данные лимиты для обеспечения соответствия с внутренними политиками и требованиями Клиента, включая, но не ограничиваясь, такими документами, принятыми Советом директоров Клиента либо равноценными документами;

Қолжетімділікті және пайдаланушылардың (соның ішінде Қауіпсіздік әкімшілердің өздерінің) құқықтарын ұсыну және ағымдағы қолдау көрсету, соның ішінде мынадай функциялар: (a) Пайдаланушының профильдерін (соның ішінде Қауіпсіздік әкімшілерінің профильерін) орнату, жою немесе өзгерту және өкілеттіктер табыстау (пайдаланушының аты жеке басын куәландыратын құжаттардағымен бірдей болуы тиіс екендігіне назар аударыңыз); (b) жеке пайдаланушыларға қолжетімді болып табылатын функциялар мен деректерді белгілейтін қолжетімділік профильдерін орнату; (c) кіру есепке алу деректерін қосу және жою; және (d) транзакциялық лимиттерді орнату (бұл лимиттер Банкпен бақыланып, бекітілмейтініне және Клиент бұл лимиттерді Клиенттің ішкі саясаттары мен талаптарына, соның ішінде, бірақ Клиенттің Директорлар кеңесімен қабылданған құжжатарымен немесе ұқсас құжаттарымен шектелмей, сәйкестігін қамтамасыз ету үшін бақылауға тиісті екеніне назар аударыңыз);

5.2 Creating and modifying entries in Customer maintained libraries (such as preformatted payments and beneficiary libraries) and authorizing other users to do the same;

Создание и изменение записей в поддерживаемых Клиентом библиотеках данных (таких как шаблоны платежей и библиотека бенефициаров), а также предоставление разрешений другим пользователям делать то же самое;

Клиент қолдау көрсететін деректер кітапханасындағы жазуларды (төлемдер шаблондары және бенефициарлар кітапханасы сияқты) орнату және өзгерту, сондай-ақ басқа пайдаланушыларға аталған әрекеттерді жүзеге асыруға рұқсат беру;

5.3 Modifying payment authorization flows;

Изменение последовательности авторизации (одобрения) платежей;

Төлемдерді түпнұсқаландырудың (мақұлдаудың) реттілігін өзгерту;

5.4 Allocating dynamic password credentials or other system access credentials or passwords to the Customer's users;

Присвоение динамического идентификатора или паролей доступа к системе для пользователей Клиента;

Клиенттің пайдаланушыларына динамикалық сәйкестендіргішті немесе жүйеге қолжетімділік үшін құпиясөздерді ұсыну;

5.5 Notifying the Bank, if there is any reason to suspect that security has been compromised; and

Уведомить Банк, если есть любые основания подозревать, что безопасность была нарушена; и

Қауіпсіздік бүлінгені жөнінде кез келген күмән туындаған жағдайда Банкті хабардар ету; және

5.6 Managing and procuring digital certificates and authorizing other users to do the same.

Управление и получение цифровых сертификатов и передачу другим пользователям полномочий для выполнения тех же действий.

Цифрлық сертификаттарды басқару және сатып алу және басқа пайдаланушыларға да солай істеуге рұқсат беру.

Please note: Security Manager roles and responsibilities may vary or not be applicable in certain markets due to regulatory requirements and/or operational capabilities. In such markets, the Bank may require additional documentation and other information from the Customer to perform Security Manager functions on behalf of the Customer.

Пожалуйста, обратите внимание: Функции и обязанности Администратора безопасности могут варьироваться или быть не применимы на территории некоторых рынков ввиду регуляторных требований и/или операционных возможностей. На таких рынках Банк может потребовать дополнительную документацию и иную информацию от Клиента для осуществления Администратором безопасности своих функций от имени Клиента.

Назар аударуыңызды өтінеміз: Қауіпсіздік әкімшілерінің функциялары реттеуші талаптарға және/немесе операциялық мүмкіндіктерге байланысты әр түрлі болуы мүмкін немесе кейбір нарықтар аумағында қолданылмайтын болуы мүмкін. Сондай нарықтарда Қауіпсіздік әкмшісімен Клиенттің атынан өз функцияларын орындау үшін Банк Клиенттен қосымша құжаттар мен өзге ақпаратты талап етуі мүмкін.

6. Use of CitiDirect and CitiConnect by Security Managers *Использование CitiDirect и CitiConnect Менеджерами по безопасности* Қауіпсіздік менеджерлерінің CitiDirect және CitiDirect-ті пайдалануы

The Bank requires two (2) separate individuals to input and authorize instructions; therefore, a minimum of two Security Managers are required. Any two Security Managers, acting in concert, are able to give instructions and/or confirmations through the connectivity channels in relation to any Security Manager function or in connection with facilitating communications. Any such communications, when authorized by two Security Managers, will be accepted and acted on by the Bank and deemed to be given by the Customer. The Bank recommends the designation of at least three Security Managers to ensure adequate backup. The Customer shall designate Customer's Security Managers on the TTS Channels Onboarding Form. A Security Manager of the Customer may also act as the Security Manager for a third party entity (for instance, an affiliate of the Customer) and exercise all rights relating thereto (including the appointment of users for that third party entity's Account(s)), without any further designation, if that third party entity executes a Universal Access Authority form (or such other form of authorization acceptable to the Bank) granting the Customer access to its account(s). This only applies in relation to Account(s) covered under the relevant authorization.

Банку необходимо два (2) человека для ввода и авторизации инструкций; поэтому требуется, как минимум, два Администратора безопасности. Любые два Администратора безопасности, действуя согласованно, могут давать инструкции и / или подтверждения через каналы связи в отношении любой функции Администратора безопасности или для содействия обмену информацией. Любые такие Сообщения, если они авторизованы двумя Администраторами безопасности, будут приниматься и исполняться Банком и считаться поручениями Клиента. Банк рекомендует назначить не менее трех Администраторов безопасности для обеспечения взаимозаменяемости. Клиент назначает своих Администраторов безопасности, используя Форму на подключение к Каналам TTS. Администратор безопасности Клиента также может действовать в качестве Администратора безопасности для компаний-третьих лиц (например, аффилированного предприятия Клиента) и осуществлять все связанные с этим права (включая назначение пользователей для Счета(-ов) такой компании-третьего лица), без какого-либо дополнительного назначения, если такая компания-третье лицо подпишет форму Разрешения на предоставление универсального доступа (или любую другую форму авторизации доступа, приемлемую для Банка), предоставляя Клиенту доступ к его счету(-ам). Это применяется только в отношении Счета(-ов), на которые распространяется в соответствующее разрешение.

Банкке нұсқаулықтардың енгізіп, авторландыру үшін екі (2) адам қажет; сондықтан кемінде екі Қауіпсіздік әкімшісі қажет болады. Келісілген түрде әрекет ете отырып, кез келген екі Қауіпсіздік әкімшісі Қауіпсіздік әкімшісінің кез келген функциясына қатысты немесе ақпарат алмасуға көмек көрсету үшін байланыс каналдары арқылы нұсқаулықтар және/немесе растаулар ұсына алады. Кез келген сондай Хабарламалар, егер олар екі Қауіпсіздік әкімшісімен авторландырылған болса, Банкпен қабылданып, орындалатын болсады және Клиенттің тапсырмасы болып саналады. Банк өзара алмасуын қамтамасыз ету мақсатында кемінде үш Қауіпсіздік әкімшісін тағайындауға кеңес береді. Клиент TTS Каналдарына қосылуға арналған Нысанды қолдана отырып өзінің Қауіпсіздік әкімшілерін

тағайындайды. Үшінші тұлға-компания Клиентке өзінің шотына(тарына) қолжетімділік ұсына отырып Әр жақты қолжетімділікті ұсынуға рұқсат нысанына (немесе Банк үшін қолайлы болып табылатын, қолжетімділікті авторландырудың кез келген басқа нысанына) қол қоятын болса, Клиенттің Қауіпсіздік әкімшісі қандай да қосымша тағайындауынсыз сондай-ақ үшінші тұлғалар-компаниялар (мысалы, Клиенттің аффилиирленген кәсіпорны) үшін Қауіпсіздік әкімшісі ретінде әрекет ете алады және сонымен байланысты барлық құқықтарды (соның ішінде сондай үшінші тұлға-компанияның Шоттына(тарына) пайдаланушыларды тағайындауды) жүзеге асыра алады. Бұл сәйкес рұқсат қатысты Шотқа(тарға) қолданылады.

7. Use of CitiDirect by Security Officers (For Personal Certificates only)
Использование CitiDirect Сотрудниками по безопасности (только для Персональных сертификатов)
CitiDirect-ті Қауіпсіздік қызметкерлерінің пайдалануы (тек жеке куәліктер үшін)

The Bank requires two (2) separate individuals to manage digital certificates attributed to individuals ("Personal Certificates"). Therefore, two Security Officers are required to assign and remove Personal Certificates to users, for the purpose of authenticating and authorizing Communications on the connectivity channels. The Bank recommends the designation of at least three Security Officers to ensure adequate backup. Any Communications authorized by Personal Certificates will be accepted and acted on by the Bank and deemed to be given by the Customer.

Банку необходимо два (2) отдельных человека для управления персональными сертификатами, которые приписываются физическим лицам ("Персональные сертификаты"). Тем самым, два Офицера безопасности должны присваивать пользователям и лишать их Персональных сертификатов для целей аутентификации и авторизации Сообщений по каналам связи. Банк рекомендует назначить не менее трех Офицеров безопасности для обеспечения взаимозаменяемости. Любые Сообщения, если они авторизованы Персональными сертификатами, будут приниматься и исполняться Банком и считаться поручениями Клиента.

Банкке жеке тұлғаларға ұсынылатын дербес сертификаттарды («Дербес сертификаттар») басқару үшін екі (2) бөлек адам қажет. Сонымен, екі қауіпсіздік офицері байланыс каналдары арқылы жолданылатын Хабарламаларды түпнұсқаландыру және авторландыру мақсаттары үшін пайдаланушыларға Дербес сертификаттарын ұсынып, оларды жоюға тиісті болады. Банк өзара алмасуын қамтамасыз ету мақсатында кемінде үш Қауіпсіздік офицерін тағайындауға кеңес береді. Кез келген Хабарламалар, егер олар Дербес сертификаттармен аворландырылған болса, Банкпен қабылданып, орындалатын болады және Клиенттің тапсырмасы ретінде саналатын болады.