SABLIER LABS LIMITED — RISK NOTICE

This Risk Notice is made available by Sablier Labs Limited **("we", "us", "ours").**

Sablier is a decentralized peer-to-peer protocol (the "Protocol") intended to allow people to distribute cryptographic assets that follow the Ethereum Token Standard (ERC-20) ("tokens"). There are four versions of the Protocol (v1.0, v1.1, v2.0, and v2.1), each of which is made up of free, public, open-source or source-available software including a set of smart contracts that are deployed on Ethereum and other EVM blockchains.

Although Sablier contributed to the initial code for the Protocol, it does not provide, own, or control the Protocol, which is run by smart contracts deployed on the relevant blockchains. Sablier has the limited governance functions for the Protocol listed here: https://docs.sablier.com/concepts/governance. It is not possible to upgrade or modify the Protocol. You should note that, just as you can access email protocols such as SMTP through multiple email clients, you can access the Protocol through dozens of web or mobile interfaces.

Accordingly, while you may use our site and services to interact with the Protocol, we cannot, and do not, represent or give any other assurance that the Protocol works in any particular way, is free of defects, or will produce the results you expect. Any documentation or other material we provide is for general information only and should not be relied upon.

To the extent we have contributed code or documentation in relation to the Protocol, the foregoing are made available "AS IS" and you use them at your own risk, without warranty from us of any kind. We are not responsible for any losses, claims or damages arising from or associated with your use, inability to use, or your interaction with other users of, the Protocol including any direct, indirect, incidental, special, exemplary, punitive or consequential damages, or loss of profits, cryptoassets, tokens, or anything else of value, save where any such liability cannot be limited or excluded by law.

Please consider the following risk factors (many of which are specific and inherent to distributed ledger technology and cryptographic assets) before accessing or otherwise using the Protocol (whether through our site and services or otherwise) as the value of tokens as well as your ability to access and transfer tokens could be materially and adversely affected if any of these risk factors materialize. As a result, when you access and/or use the Protocol, you expose yourself to potential losses.

Please note this Risk Notice is not exhaustive. Before using the Protocol, you should review the relevant documentation (including the smart contract code which is publicly accessible) to make sure you understand how the Protocol works, and you should carry out further research (and seek professional advice) to carefully determine whether using the Protocol is suitable for your particular circumstances and risk tolerance.

RISK ASSOCIATED WITH PROTOCOLS: Tokens are recorded on distributed ledgers (typically shared across networks of users) which are governed by, subject to, and distinguished on the basis of certain set of rules known as protocols. When you use the Protocol, you are exposed to the following risks: **(i) Malfunction, breakdown and/or abandonment of protocols -** Any malfunction, breakdown, and/or abandonment of the protocols (and of any underpinning consensus mechanism) on which the tokens are based could severely affect the price of the tokens as well as your ability to dispose of the tokens (particularly where the protocol relies on substantial participation and wide networks to operate properly); **(ii) Mining attacks -** Some protocols integrate consensus-based mechanisms for the validation of transfers. Consensus protocols are susceptible to attacks at the stage of validation, where

transactions are approved by the network. This may affect the accuracy of transactions occurring on the protocol, and result in tokens being misappropriated (for example, through what is typically referred to as double spending attacks); and **(iii) Hacking and security weaknesses -** Tokens may be subject to expropriation and/or theft. Bad actors (such as hackers) may attempt to interfere with protocols or tokens in a variety of ways, including, but not limited to, malware attacks, denial of service attacks, consensus-based attacks, sybil attacks, smurfing and spoofing. Furthermore, some protocols are based on open-source software and, as a result, are subject to the risk of weaknesses being introduced to the protocols (either willingly or accidentally) at the development stage. Any such weakness may be exploited by bad actors for the purposes of misappropriating tokens, or otherwise affect the functionality of the protocol and your ability to retain control of tokens.

LACK OF PROTECTION: The Financial Services Compensation Scheme (FSCS) doesn't protect you from losses incurred if something goes wrong here as it is not covered for protection under the UK regulatory regime; in other words, it isn't recognized as something that the FSCS can protect. The Financial Ombudsman Service (FOS) will not be able to assist you either in relation to any losses that might occur should something go wrong.

PRICE VOLATILITY: Your use of the Protocol involves various risks, including, but not limited to, losses to the fluctuation of the prices of tokens during the time that you are streaming tokens through the Protocol, due to the rapid shifts in supply and demand resulting from events including but not limited to: (a) good or bad publicity, (b) changes in the financial technology industry, (c) technological advancement, (d) market trends, (e) general economic and/or political conditions, (f) degree of adoption, (g) degree of institutional support, (h) regulatory measures, (i) degree of government support, (I) market dynamics, (m) trading activities, (n) hacking, and (o) events affecting large service providers, including exchanges. As a result of price volatility, tokens may lose some or all value.

SECURITY: Tokens are stored (or recorded against) cryptographic wallets **("Wallets").** A private key (for example, a passphrase) is usually necessary to access, control and/or dispose of tokens that are stored in your Wallet. Note that we do not hold copies of your private key(s), and you are solely responsible for implementing all reasonable and appropriate measures for securing access to your private key(s) and Wallet. Losing access to the private key(s) associated with your Wallet may result in the permanent loss of your ability to access and dispose of tokens.

THIRD PARTIES: We have no control over the provision or your use of third-party products and services to interact with the Protocol. You are responsible for undertaking your own diligence on those services to understand the associated fees and risks.

CHANGES IN THE LEGAL AND REGULATORY FRAMEWORK APPLICABLE TO DISTRIBUTED LEDGER TECHNOLOGY: The legal and/or regulatory framework surrounding tokens and distributed ledger technology is uncertain, not harmonized, and unsettled in many jurisdictions. It is difficult to predict what framework will become applicable to distributed ledger technology and tokens in the near future and how the implementation of dedicated legal and/or regulatory frameworks will affect the price, legality, or utility of tokens. A newly introduced legal and regulatory framework may interfere with or otherwise limit your ability to access and use the Protocol, which in turn may result in a financial loss.

TAXATION: The tax characterization of tokens is complex and largely uncertain. The uncertainty in the tax treatment of tokens may expose you to unforeseen future tax consequences associated with the use of the Protocol (particularly when you stream cryptographic assets through the Protocol). You should seek tax advice to understand what tax obligations apply to you when using cryptographic

assets in connection with the Protocol. Failure to comply with your tax obligations could amount to a criminal offense.