Exhibit 1-A

In re LastPass Data Security Incident Litig., No. 1:22-cv-12047-PBS (D. Mass.)

Confidential Cryptocurrency Theft Claims Process

As part of this process, Claimants will be given a secure way to provide the information below to Special Master Bruce Friedman, who, together with the Cryptocurrency Loss Expert, will agree to abide by security and confidentiality requirements in order to keep the below information secure and not disclose it to unauthorized third parties.

Basic Claimant Information
Name, Social Security number, email address used to access your LastPass vault(s), and email address used to interact with your cryptocurrency assets on the impacted wallet, if different than your LastPass email.
Prima Facie Showing (Claimant Supplied Information)
Claimants to Provide Verified Answers to Following Questions: [1] **[*The information provided by a claimant in response to the questions below will be considered in a totality-of-the-circumstances fashion, and the inability of a claimant to answer any one or more of these questions shall not alone be fatal to the claim*]** 1. What type(s) of cryptocurrency was/were stolen and in what amount(s)? 2. What is/are the date(s) of theft and approximately when did you first discovery it/them? 3. What type(s) of cryptocurrency wallet(s) was/were used to store your stolen cryptocurrency, and what is the address for each? What is/are the address(es) of the wallet(s) where your stolen cryptocurrency was sent? 4. Do you have documents or screenshots showing the balance of your compromised wallet(s) before and after the theft(s)? If yes, please provide copies. 5. Are you the sole owner of the compromised wallet(s)? If not, identify all other owners. 6. Do you know the date(s) (or approximate date(s)) when you created the private key(s)/seed phrase(s) for the compromised wallet(s)? If so, please provide. 7. Identify or describe all places where you stored your private key(s)/seed phrase(s) for the compromised wallet(s)? 8. If you stored your private key(s)/seed phrase(s) for your compromised wallet(s) in your LastPass vault, did you store them in your vault before September 16, 2022? 9. Did anyone other than you have access to the private key(s)/seed phrase(s) for your compromised wallet(s)? If yes, identify everyone who had access. 10. Do you have transaction records, blockchain data, or other information you believe may be relevant or related to the fraudulent transactions. This may include, but is not limited to: transaction IDs (hashes), Bitcoin address outputs and/or IP addresses, for the theft(s) from your compromised cryptocurrency wallet(s). If yes, please provide copies. 11. Did you report the theft(s) to law enforcement (e.g., local police, the FBI and/or IC3 (the Internet Crime Complaint Center))? If yes, when did you make the report? Was a written report

[1] For the avoidance of doubt, claimants may be assisted by class counsel or their own counsel in compiling data to support their individual claims.

created/submitted? If you retained a copy of the written report, please provide it. If you made a report, what is the status of law enforcement's investigation (if you know)?

12. Have you sought and/or received reimbursement for this/these theft(s) from any other source? If yes, please identify from whom and when you sought reimbursement, and how much (if anything) you received in reimbursement.
13. In the last four years, have you observed any attempted or successful logins to your cryptocurrency exchange or bank/credit card or core/cloud (Google, Apple, Dropbox, iCloud, etc.) accounts: yes or no? If yes and you recall details of such logins or attempts, please provide additional information.
14. *Other than this claim*, in the last four years, have you been the victim of any identity-related (including financial or cryptocurrency) theft or fraud: yes or no? If yes and you recall details of such theft or fraud, please provide additional information, including whether you suffered any monetary losses and were reimbursed for such losses.
15. What types of computing devices (e.g., Android or iOS smartphones or tablets, Windows-based PC) and applications or browsers (e.g., web-enabled wallets) did you use to access or transact with your compromised cryptocurrency wallet(s)?
16. In the last four years, has any info-stealer-type malware been detected on any computing devices you use, including personal computers, tablets, and mobile devices: yes or no? If yes and you recall details of such malware, please provide additional information.
17. Before September 2022, did you store *other* private key(s)/seed phrase(s) (meaning other than the compromised wallet which is the subject of this claim) or financial or cryptocurrency account login credentials in your LastPass vault? If so, to your knowledge, has any of that information been misused?
18. Identify everywhere you keep or store your master password to your LastPass account.
19. How did (or do) you remember your master password?
20. Have you ever shared your master password with anyone? If yes, who?
21. Is your master password to your LastPass account the same password you use for any other accounts or logins you have? If yes, how many times have you reused your master password and for what types of accounts or sites (if you recall)?
22. Is there anything else that you think is important for the Special Master to know about your claim? If yes, please explain.

Prima Facie (Special Master Determination)

The Special Master shall select a technical expert/consultant to assist with reviewing claimant submissions and any rebuttal submissions (the "Cryptocurrency Loss Expert"). The Cryptocurrency Loss Expert shall have significant experience with forensic analysis of blockchain/cryptocurrency theft.

Based on the verified responses and information provided by claimant, the Special Master determines if the claim meets a prima facie showing and should be subject to further review.

Special Master Confirmation (After Prima Facie Showing)

If the Special Master determines that the claimant made a prima facie showing, the Claimant then provides their master password (if known) to open the forensically preserved copy of the exfiltrated

backup copy of the instance of the claimant's LastPass vault to validate that the compromised wallet private key(s)/seed phrase(s) were stored in the secure notes folder at time of the incident.

At this phase, claimants will be asked: Have you changed your master password to your LastPass vault since September 2022? If no, what is your master password? If yes, do you recall your master password around or before September 2022? If yes, please provide it.

Claimants whose compromised wallet private keys/seed phrases are confirmed as having been stored in the backup copy of their vaults will be considered "Tier 1 Claimants."

Claimants whose compromised wallet private keys/seed phrases are confirmed as not having been stored in the backup copy of their vaults will have their claims rejected as invalid/denied with no further adjudication.

Claimants who cannot recall their master password to open the backup copy of their vaults will be considered "Tier 2 Claimants."

The Special Master shall continue to adjudicate Tier 1 Claimants' claims until final resolution of them.

In the interim, Tier 2 Claimants will be subject to requests for additional forms of proof by the Special Master to verify that their compromised wallet private keys/seed phrases were actually stored in their LastPass vaults at the time of the incident. The Special Master, in coordination with his expert, will develop additional confirmation criteria including posing additional questions to the claimant or LastPass to include, but not be limited to, questions about where within the claimant's LastPass vault did they store the impacted private key/seed phrase (e.g., Secure Note or within the notes section of a credential for a website, etc.).

Validation of Tier 2 Claimants will occur after final adjudication of Tier 1 Claimants.

Independent Blockchain Transaction/Cryptocurrency Theft Forensic Expert Analysis

For claims the Special Master, aided by the Cryptocurrency Loss Expert, determines a blockchain transaction report and forensic analysis would be warranted, the appointed Cryptocurrency Loss Expert shall review the blockchain for the transactions at issue and perform such analysis to confirm unauthorized movement of specific cryptocurrency out of the claimant's wallet(s) at issue during the date/times claimant contends theft occurred.

This analysis is to confirm dates and movement of unauthorized transactions relating to cryptocurrency wallet(s) at issue on the blockchain, including any information that may connect the thefts to the LastPass Incident or another source of compromise.

The analysis will be based on all publicly available data on the blockchain about the transaction(s) at issue.

The Special Master and the Cryptocurrency Loss Expert will be solely responsible for analyzing the blockchain data and making any reasonable inferences or drawing conclusions, if any, from the data.

The Special Master and the Cryptocurrency Loss Expert will analyze blockchain data for all Tier 1 Claimants prior to making individual determinations with respect to each Tier 1 Claimant's claim. The Special Master and the Cryptocurrency Loss Expert will analyze blockchain data for all validated Tier 2 Claimants prior to making individual determinations with respect to each validated Tier 2 Claimant's claim.

The Special Master, with the assistance of the appointed Cryptocurrency Loss Expert, will consider the analysis as a set of data points to be considered in a totality-of-the-circumstances approach, and the absence of any one data point shall not necessarily be determinative.

Additional Data Points (Optional)

At their discretion, either LastPass or the claimant *may* supplement the record with the following information:

- Documentation of suspicious login attempts to claimant's LastPass account during relevant time periods.
- The iteration count setting for claimant's LastPass vault at time of the incident, including applicable rainbow tables.
- Third party threat intelligence reports relating to the email address associated with claimant's LastPass account and/or passwords or other PII found in other data breaches, on the dark web, and/or on infostealer sites.
- A list of associated URLs for the claimant's vault (based on the forensic copy).

At his discretion, the Special Master may ask either LastPass or Claimant to provide the above-described data or, without limitation, other data available to the parties.

Final Adjudication (by Special Master)

The Special Master, as assisted by the appointed the Cryptocurrency Loss Expert, will review all of the evidence in the record for claimant's claim and determine whether the LastPass incident was the cause of the claimant's cryptocurrency loss and, if so, the amount of such loss to be recovered. The Special Master shall apply a preponderance of evidence (i.e., more likely than not) standard.

The final determination by the Special Master shall be confidential, regardless of outcome, and shall not be subject to requests for reconsideration or appealable.

If a claim is approved, in whole or in part, the Special Master will only report to the claimant the amount of their approved claim, including, if applicable, an explanation of any pro rata reduction.

If a claim is rejected, the claimant will be informed that their claim has been rejected due to insufficient or lack of supporting evidence relating their loss to the LastPass Data Incident.

The Special Master's and the Cryptocurrency Loss Expert's working files, analyses, and bases for decisions shall remain confidential and not disclosed to claimant or LastPass. Upon final

adjudication of a claim, the Special Master and the Cryptocurrency Loss Expert will delete or destroy all files related to that claim.