Draft Cybercrime (Jersey) Law 201-

Written Submission – European Bank operating in Jersey – 19 November 2018

1. Generally, the Draft Cybercrime (Jersey) Law 201- ("**Draft Law**") is a positive step in order to keep Jersey up-to-date and moving forward in respect of technological advancement. The concern for banks, who might be considered obvious targets of alleged unauthorised use and access contained in the Draft Law, will likely be around preservation orders and ensuring they have the requisite controls in place should orders be issued.

2. More specifically, around formatting (the order of amendments), it may be more helpful to include the amendment included in Article 1(2)(b) of the Draft Law straight after Article 1(5) of the Computer Misuse (Jersey) Law 1995 ("**CML**") as both discuss 'unauthorized' acts and access respectively.

3. Also specifically, for the benefit of consistency and clarity, Article 1(2) (b) of the Draft Law may need to include the wording 'who is so entitled' after Article (8)(b) to be included in the CML.

4. Page 7 Investigation of encrypted data (Article 19) - We encrypt communication flows and application access with industry standard certificates/protocols which may be tied to a user, recreating this access for a request for the data may require some time. The new draft law is not very specific in what it classes as a "timely manner". As this is very similar to the data discovery process under the Jersey implementation of GDPR (where a set time frame is given of 30 days), could a similar defined timeframe not be given to manage the expectations of everyone involved.

5. Page 20 Section 5D(4) - Can we clarify that to what level we can disclose any request for information under this law to "within the Group". I.e. we may well need to explain why we are asking for snapshots of data or to ensure data is ring-fenced from data purging or modification to other Group members. In addition to this what is the position in informing third parties outside of the Group if similar ring-fencing or data discovery is required for data stored on a third party infrastructure.

6. Page 21 Section 3(2)1(A) (C) - Does this refer to cloud services and/or cloud storage, my interpretation is that it does and we should bear this in mind when we allow access to such cloud services to either users or as part of business applications that use cloud services.