Appendix

Program change for GDPR

Your Agreement is hereby supplemented and amended as follows:

The "Data Protection" section in Schedule B of the Agreement (or equivalent) shall be deleted and replaced with the following, and shall be re-numbered accordingly. Any reference to Schedule A shall mean the equivalent terms within your Agreement:

6. Data Protection – In so far as the Bank or any of its Affiliates is subject to: (i) the EU Directive on Data Protection (95/46/EC) and the EU Directive on Privacy and Electronic Communications (2002/58/EC); (ii) any national laws implementing such directives; (iii) when applicable, the General Data Protection Regulation (EU) 2016/679 and any laws or regulations implementing or made pursuant to such regulation (the "GDPR"); and (iv) the laws and/or regulations of any country outside the European Economic Area ("EEA") that are intended to provide equivalent protections for Personal Data (or the nearest equivalent term under applicable data protection laws and/or regulations) of Data Subjects as the GDPR, including without limitation, the data protection laws of Jersey, Switzerland and the United Kingdom ("Equivalent Law") in relation to any Personal Data Processed in connection with the Program, the following sections in Schedule A are amended as follows (and for the avoidance of doubt all such laws and regulations shall be deemed to be included within the definition of "Data Protection Laws" for purposes of the application of this Schedule B):

6.1 In section 12(a) of Schedule A, the following definition shall replace section 12(a)(iii):

"(iii) "Personal Data" means any information that can be used, directly or indirectly, alone or in combination with other information, to identify a Data Subject or, if different, the meaning given to this term or nearest equivalent term under applicable Data Protection Laws, and includes any or all of Bank Personal Data, Company Personal Data and Cardholder Personal Data, as the context requires;

(A) "Bank Personal Data" means Personal Data relating to employees, partners, officers, contractors, agents and subcontractors of the Bank and/or any Bank Affiliates received, accessed and/or otherwise Processed by the Company or any Participating Affiliates in connection with the Program;

(B) "Cardholder Personal Data" means Personal Data relating to Cardholders received, accessed and/or otherwise Processed by the Bank or any Bank Affiliates in connection with the Program;

(C) "Company Personal Data" means Personal Data relating to Cardholders, employees, partners, officers, contractors, agents and subcontractors of the Company and/or any Participating Affiliates received, accessed and/or otherwise Processed by the Bank or any Bank Affiliates in connection with the Program;

6.2 In section 12(a) of Schedule A, the following clause is added to the definition of "Permitted Purposes" in section 12(a)(iv):

"and (L) any additional purposes as may be notified to the Company or Data Subjects in any notice provided pursuant to section 12(i) of Schedule A;"

6.3 In section 12(a) of Schedule A, the following new definitions are inserted:

"(vi) "Data Controller" means the natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of Personal Data, or if different, the meaning given to this term under applicable Data Protection Laws;

"(vii) Data Subject" means a natural person who is identified, or who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity, or, if different, the meaning given to this term or nearest equivalent term under applicable Data Protection Laws."

6.4 The following text is added to the end of section 12 (i) of Schedule A:

Notwithstanding the previous sentence, to the extent that the Processing of Personal Data is subject to the GDPR or any Equivalent Law, the Company warrants that it shall provide: (i) the relevant Data Subjects with a copy of the TTS Commercial Cards Privacy Statement accessible at https://www.citibank.com/tts/docs/TTS_Commercial_Cards_EEA_Privacy_Statement.pdf (or such other URL or statement as the Bank may notify to the Company from time to time); (ii) any additional notice(s) to, and shall seek consent from, the relevant Data Subjects in relation to the Bank's and other Processing Entities' Processing of their Personal Data in accordance with any instructions of the Bank from time to time (which may include the form and the manner in which a notice is to be provided, or any consent is to be obtained) to the extent such notices and/or consents are required under applicable Data Protection Laws; and (iii) promptly to the Bank upon the Bank's request, evidence of having provided such statements, notices and/or obtained such consents.

6.5 In section 12(j), the following new subclauses are inserted:

"(iii) Without limiting section 12(j)(i), to the extent that the Processing of Personal Data is subject to the GDPR or any Equivalent Law, the Company shall ensure that any Company Personal Data that it provides to the Bank has been Processed fairly and lawfully, is accurate and is relevant for the purposes for which it is being provided and the Bank may rely on the Company's compliance with such undertaking and, where applicable, assistance from the Company pursuant to Section 12(i) (Legal Basis for Processing). Each party acknowledges that it is a Data Controller in relation to the Personal Data that it Processes in connection with this Agreement.

(iv) The Company acknowledges that pursuant to section 12(d), Cardholder Personal Data may be disclosed to Representatives located in countries outside the EEA which do not offer an adequate level of protection (as the term is used in Data Protection Laws applicable in the EEA). In relation to such disclosures, the Bank acknowledges that it is responsible for complying with the data transfer rules set forth in Data Protection Laws applicable in the EEA including (where deemed appropriate by the Bank) through the execution of standard contractual clauses in the form adopted or approved by the European Commission.

(v) Upon request, the Bank will provide the Company with a list of third parties appointed by the Bank to process Cardholder Personal Data on the Bank's behalf in connection with the Program. The Bank acknowledges that as a Data Controller established in the United Kingdom, the Bank is responsible for ensuring that the processing of Cardholder Personal Data by such third parties is compliant with Data Protection Laws applicable in the United Kingdom.

(vi) The Bank shall provide the Company with such information as is reasonably requested by the Company to enable the Company to satisfy itself of the Bank's compliance with its obligations under this section 12(j). Nothing in this section shall have the effect of requiring the Bank to provide information that may cause it to breach its confidentiality obligations to third parties."

TTS COMMERCIAL CARDS PRIVACY STATEMENT

Citi's Treasury and Trade Solutions (TTS) commercial cards business provides commercial cards programs to corporations, financial institutions and public sector organizations (this Privacy Statement refers to each of these as the "Company"). This Privacy Statement explains how this business processes personal data about people with whom we come into contact (referred to as "you" in this Privacy Statement) in the course of our dealings with the Company and other relevant persons. This includes individuals to whom the Company has requested Citi to issue a card ("Cardholders"), as well as employees, officers, directors and other personnel of the Company, service providers and other business counterparties (referred to as "Your Organization" in this Privacy Statement).

1. Who is responsible for your personal data and how can you contact them?

The Citi entities listed here (referred to as "we" in this Privacy Statement) are the controllers of your personal data:

• Citibank Europe Plc., UK Branch, Citigroup Centre, Canada Square, Canary Wharf, London, E14 5LB, United Kingdom. Telephone +44 20 7500 5000

For further detail you may contact our Data Protection Officer at dataprotectionofficer@citi.com or Citigroup Centre, 33 Canada Square, Canary Wharf, London E14 5LB, United Kingdom.

2. Why do we process your personal data?

We process your personal data, as necessary to pursue our legitimate business and other interests, for the following reasons:

- to provide a commercial cards program to the Company and Cardholders and to communicate with the Company and Cardholders about the program;
- to manage, administer and improve our business and Company and service provider engagements and relationships, for corporate marketing, business development and analysis purposes and to operate control and management information systems;
- to monitor and analyze the use of our commercial cards programs for system administration, operation, testing and support purposes;
- to manage our information technology and to ensure the security of our systems;
- to establish, exercise and/or defend legal claims or rights and to protect, exercise and enforce our rights, property or safety, or to assist the Company or others to do this; and
- to investigate, respond to and deal with complaints or incidents relating to us or our business, to maintain service quality and to train staff.

We also process your personal data to comply with laws and regulations. We sometimes go beyond the strict requirements of the relevant law or regulation, but only as necessary to pursue our legitimate interests in cooperating with our regulators and other authorities, complying with foreign laws, preventing or detecting financial and other crimes and regulatory breaches, and protecting our businesses and the integrity of the financial markets. This involves processing your personal data for the following reasons:

- to cooperate with, respond to requests from, and to report transactions and/or other activity to, government, tax or regulatory bodies, or other intermediaries or counterparties, courts or other third parties;
- to monitor and analyze the use of our products and services for risk assessment and control purposes (including detection, prevention and investigation of fraud);
- to conduct compliance activities such as audit and reporting, assessing and managing risk, maintenance of accounting and tax records, fraud and anti-money laundering (AML) prevention and measures relating to sanctions and anti-terrorism laws and regulations and fighting crime. This includes know your customer (KYC) screening (which involves identity checks and verifying address and contact details), politically exposed persons screening (which involves screening client records against internal and external databases to establish connections to 'politically exposed persons' (PEPs) as part of client due diligence and onboarding) and sanctions screening (which involves the screening of clients and their representatives against published sanctions lists); and

- to record and/or monitor telephone conversations so as to maintain service quality and security, for staff training and fraud monitoring and to deal with complaints, disputes and potential and/or actual criminal activity. To the extent permitted by law, these recordings are our sole property.

In most cases we do not rely on consent as the legal basis for processing your personal data. If we do rely on your consent, we will make this clear to you at the time we ask for your consent.

If you do not provide information that we request, we may not be able to provide (or continue providing) relevant products or services to or otherwise do business with you or Your Organization.

3. Services alerts

Cardholders will automatically receive service update alerts from us by post or email where contact details have been provided by the Company. You will be able to opt in to receive such alerts by SMS and to receive other alerts by email by registering with CitiManager, which is a service that allows you to access and view your card statements online. Please note that, if you register for such SMS alerts, then your telecoms provider may charge you to receive such alerts if you travel abroad; we are not responsible for any such charges. If you wish to change the alerts that you receive, please do so through CitiManager or call Customer Services on the number on the back of your card.

4. Where does Citi obtain personal data about you?

We process personal data that you provide to us directly or that we learn about you from your use of our systems and our communications and other dealings with you and/or Your Organization. Your Organization and other organisations will also give us some personal data about you, including as set out below:

- ***from Your Organization***: your date of birth, nationality, title and employee ID, contact details such as your business email address, home or business address and telephone number and other information required for KYC, AML and/or sanctions checking purposes (eg, a copy of your passport);
- ***from public sources*:** information collected from international sanctions lists, publically available websites, databases and other public data sources;
- ***from the Company and its program administrators***: in the case of a Cardholder, the individuals who administer the commercial cards program on behalf of the Company, and/or the Company itself, may provide personal data relating to you, and submit change of personal data requests made by you on your behalf, to us, whether through use of an electronic card management and reporting system or otherwise. Such requests may be to update any of the information about you or your account set out in your application form, such as your name, address and email address. We may contact your manager or your program administrator about you and your account; and
- ***from merchants***: in the case of a Cardholder, merchants which accept our commercial cards and accounts will transfer information to the relevant bank card association and to us about any transactions that you make with them using your card or account.

5. To whom do we disclose your personal data?

We disclose your personal data, for the reasons set out in Section 2, as follows:

- to Your Organization and, if different, your employer, other members of the same group of companies, and authorized third parties, including, if you are a Cardholder, disclosure to program administrators and other individuals who are authorized by your Company about charges made and fees applied to your card or account, the status of your account and other data relating to your card and account, whether through use of an electronic card management and reporting system or otherwise, for the purpose of expense and travel management and administration;
- to other Citi entities (this includes the entities referenced at http://www.citigroup.com/citi/about/countrypresence/) for the purpose of managing Citi's Company, service provider and other business counterparty relationships;
- to persons from whom we receive, or to whom we make, payments on your or the Company's behalf;

- to service providers who provide services which are complementary to a commercial cards program, including application processing, fraud monitoring, call center and/or other customer services, card production and other technology and business process outsourcing services;
- to our professional service providers (eg, legal advisors, accountants, auditors, insurers and tax advisors);
- to legal advisors, government and law enforcement authorities and other persons involved in, or contemplating, legal proceedings;
- to competent regulatory, prosecuting, tax or governmental authorities, courts or other tribunals in any jurisdiction;
- to other persons, including merchants who accept our cards, where disclosure is required by law or to enable a commercial card program to be provided to you or the Company; and
- to prospective buyers as part of a sale, merger or other disposal of any of our business or assets.

6. Where do we transfer your personal data?

We may transfer your personal data to Citi entities, regulatory, prosecuting, tax and governmental authorities, courts and other tribunals, service providers and other business counterparties located in countries outside the European Economic Area (EEA), including countries which have different data protection standards to those which apply in the EEA. This includes transfers of personal data to Singapore, India and the United States of America. When we transfer your personal data to Citi entities, service providers or other business counterparties in these countries, we will ensure that they protect your personal data in accordance with EEA-approved standard data transfer agreements or other appropriate safeguards.

7. How long do we keep your personal data?

We keep your personal data for as long as is necessary for the purposes of our relationship with you or Your Organization or in connection with performing an agreement with the Company or Your Organization (if Your Organization is not the Company) or complying with a legal or regulatory obligation.

8. What are your rights in relation to personal data?

You can ask us to: (i) provide you with a copy of your personal data; (ii) correct your personal data; (iii) erase your personal data; or (iv) restrict our processing of your personal data. You can also opt out of the processing of your personal data for direct marketing purposes or object to our other processing of your personal data. These rights will be limited in some situations; for example, where we are required to process your personal data by EU or EU member state law.

To exercise these rights or if you have questions about how we process your personal data, please contact us using the contact details in Section 1. We can in particular provide copies of the data transfer safeguards referred to in Section 6. You can also complain to the relevant data protection authorities, in the EEA member state where you live or work or where the alleged infringement of data protection law occurred.

9. Changes to this Privacy Statement

This Privacy Statement takes effect on 25 May 2018; it was last updated on 25 May 2018. If we change it, to keep you fully aware of our processing of your personal data and related matters, we will post the new version to this website.