Supplier Invoicing Guidelines

Below are guidelines for how JPMorgan Chase does business with suppliers. These guidelines may occasionally change, and suppliers agree to remain in compliance with the updated terms. Violation of these guidelines may be considered a material breach of agreement.

INITIAL SET-UP

1. Electronic Invoicing

JPMorgan Chase requires electronic invoicing through the Ariba Supplier Network or Supplier Central Digital Invoicing for select locations Click here to see the list of locations where electronic invoicing is required. Suppliers can register for an Ariba Enterprise account or Standard account to submit invoices electronically. Please visit https://www.ariba.com/ariba-network/ariba-network-for-suppliers for further information. Any associated fees are the responsibility of the supplier and should not be charged back to JPMorgan Chase. Once a supplier is enabled with Ariba, paper invoices will be rejected and sent back for electronic re-submission. Invoices submitted outside the Ariba Supplier Network (e.g., via email or fax) are NOT considered electronic.

When submitting invoices via Ariba, suppliers are required to issue a separate invoice per ship-to location in order for tax validation and calculation processes to work properly in the JPMorgan Chase Ariba environment. For Supplier Central, suppliers may submit a single invoice with different ship-to locations on each item line.

JPMorgan Chase will have no obligation to pay any amounts invoiced to JPMorgan Chase 180 days or more after incurred.

2. PO Requirement

JPMorgan Chase requires all new suppliers to be approved in advance prior to transacting. Pre-approval using a purchase order (PO) is required for transactions with most suppliers. Therefore, these suppliers must receive a purchase order from JPMorgan Chase prior to delivering the goods/services. Requests for payment of such goods or services without purchase orders may not be accepted. Invoices without reference to a purchase order may experience significant delays due to spend approvals and validations.

Submitting a purchase order invoice via paper or directly to your JPMorgan Chase business contact will likely delay the invoice payment and is contradictory to our electronic invoice requirement.

Click here to see the list of locations where purchase orders are required.

3. Supplier Registration through the JPMorgan Chase Global Supplier Portal

New U.S. suppliers will be invited to register within JPMorgan Chase's Global Supplier Portal in order to be set up to conduct business with JPMorgan Chase. U.S. suppliers will receive an email with a unique user ID and temporary password to complete the registration.

Non-US suppliers will be required to work with their JPMorgan Chase contact and provide the necessary documentation required by the JPMorgan Chase Global Supplier Setup Team to complete the set up.

4. Payment Terms

JPMorgan Chase's standard payment terms are 2% 10 business days; net 60 unless different terms are negotiated under contract or mandated by law in a particular country. "2% 10" means that JPMorgan Chase will receive a two

percent discount off any fees or amounts due under any accurate invoice as long as JPMorgan Chase pays that invoice within 10 business days of receipt of the invoice and in accordance with the Schedule.

In line with standard industry practices, JPMorgan Chase calculates payment terms based upon the receipt of a fully compliant invoice including validation of goods/services received with an undisputed amount. Invoices submitted electronically via the Ariba Supplier Network (ASN) will have the payment terms calculated from the date of submission on the network.

For card payments (virtual credit card AKA 'Single Use Account'), JPMorgan Chase will issue the virtual card details for the supplier's use on an expedited basis and the standard payment terms do not apply.

5. Payment Method

JPMorgan Chase is entitled to select, at its own discretion, the payment method: (i) bank wire transfer (ACH) or (ii) card payments facilitated via a card product (e.g., single use account). JPMorgan Chase's preferred method of payment is with a virtual credit card (Single Use Account). Any associated fees are the responsibility of the supplier and should not be charged back to JPMorgan Chase. Payments made with a virtual card product will be paid on an expedited basis following invoice approval. Therefore, the payment is not subject to the standard 2%10 Net60 payment terms. In locations where card payment is unavailable, suppliers are required to receive payment electronically from JPMorgan Chase to a single bank account through ACH, BACS, etc. For example, a supplier providing multiple services cannot specify different bank accounts depending on the service in question. Suppliers that provide goods or services to different JPMorgan Chase countries can use a different bank account per country, but only one bank account per country per currency is allowed. It is the supplier's responsibility to communicate and maintain accurate banking details such as bank account #, remittance information, email address (for either card payments or single use account payments), etc. Changes to a supplier's banking information must be initiated through their JPMorgan Chase LOB contact.

To satisfy cybersecurity requirements, suppliers may receive multiple phone calls to validate settlement instructions during initial set-up, or any changes thereafter.

6. Single Currency

Suppliers are required to invoice in only one currency per JPMorgan Chase country. For example, a supplier providing goods or services to JPMorgan Chase in the UK cannot submit some invoices in Euro and other invoices in British Pounds. Suppliers that provide goods or services to multiple JPMorgan Chase countries can invoice in one currency per country. Payment currency should be either the local currency of the JPMorgan Chase entity or the local currency of the supplier.

7. Bank Charges

International supplier payments are sent on a shared charge basis. This means that JPMorgan Chase will pay any costs to send the funds, however if the supplier's bank or any intermediary bank levies charges, these will be paid by the supplier.

8. Tax Documentation & Treatment

Suppliers must submit tax documentation to JPMorgan Chase at the time of initial set-up and/or with each invoice, as required by applicable regulations. Tax documentation relating to the JPMorgan Chase country being billed, the supplier's country and/or the United States may be required. JPMorgan Chase will perform periodic reviews of supplier tax documentation and will require suppliers to provide updated documentation upon request.

Suppliers are responsible for issuing invoices which comply with all applicable rules and regulations. Suppliers should invoice the JPMorgan Chase location that is benefitting from the goods or services being provided.

ONGOING REQUIREMENTS

9. Due Diligence

Suppliers must address invoices to the JPMorgan Chase legal entity to whom goods or services have been provided, and the legal entity name and office address must be accurately stated. This should correspond to the JPMorgan Chase legal entity that a Purchase Order is issued by. Suppliers who submit electronic invoices which include JPMorgan Chase internal accounting information must work with their JPMorgan Chase contact to ensure that any cost centers correspond to the JPMorgan Chase legal entity that the invoice is addressed to. For some invoice types the bill-to legal entity is chosen via a list of Ariba reference codes. This link lists the JPMorgan Chase legal entities in each country with corresponding Ariba reference codes. Invoices with mismatching billing and accounting details will be rejected.

JPMorgan Chase conducts due diligence/anti-money-laundering/crime prevention checks throughout the life of a supplier relationship. This means that JPMorgan Chase may periodically require additional information from suppliers before we can make ongoing invoice payments as well as to initiate new supplier relationships.

In the event of an acquisition by or merger with JPMC of a legal entity with whom a supplier is doing business the supplier will become subject to these guidelines and will change their billing practices as and when requested, upon receiving formal communication from the JPMC Sourcing team.

10. Withholding

JPMorgan Chase may be required to deduct and withhold applicable tax from invoice amounts, based primarily on the character and source of the payment and the tax status of the supplier/payee, as determined by tax documentation provided by the supplier.

JPMorgan Chase is not authorized to provide tax advice to clients or counterparties. Suppliers should direct all queries to their own tax advisor or local tax authority, including questions about the kind of tax documentation required, or when withholding deductions apply.

11. Supplier Maintenance

Any supplier account with no activity for over 18 months will be required to submit new documentation if JPMorgan Chase does business with the supplier again.

12. Credit Invoices

Suppliers will submit credit invoices promptly, through the same submission process as a normal debit invoice. To ensure accurate accounting and tax reporting, credits should not be directly adjusted against subsequent invoices by the supplier. If further business with JPMorgan Chase is not anticipated, or debit invoices of sufficient value for JPMorgan Chase to offset the credit are not issued within 180 days, the supplier should consult their JPMorgan Chase contact in order to issue a refund.

13. Set-offs

JPMorgan Chase may set off any amounts owed to JPMorgan Chase under any applicable agreement against any invoices and unless the supplier disputes the set-off in writing within ten (10) business days, the supplier agrees the set-off is valid.

14. Statement and Duplicate Audit

JPMorgan Chase will engage third party suppliers and/or perform internal statement and duplicate audit on an annual basis. Suppliers are required to provide statements and other supporting documentation to perform these audits.

15. Invoice Status (U.S. suppliers only)

Suppliers can check the status of an invoice by accessing Invoice Lookup on the JPMorgan Chase website.

Purchase Orders & Electronic Invoicing by Location[1]

Location	Purchase Order Required	Electronic Invoicing Required
United States of America	Yes	Yes
United Kingdom	Yes	Yes
Argentina	Yes	No
Australia	Yes	Yes
Bahrain	Yes	Yes
Belgium	Yes	Yes
Brazil	Yes	Yes
Canada	Yes	Yes
Chile	Yes	Yes
China	Yes	Yes
Colombia	Yes	Yes
France	Yes	Yes
Germany	Yes	Yes
Hong Kong	Yes	Yes
India	Yes	Yes (Hard copy also required)
Indonesia	Yes	Yes
Ireland	Yes	Yes (Paymentech)
Italy	Yes	No
Japan	Yes	Yes
Korea	Yes	Yes
Luxembourg	Yes	Yes
Malaysia	Yes	Yes (Hard copy also required)
Mexico	Yes	Yes
Netherlands	Yes	Yes
Peru	Yes	Yes
Poland	Yes	Yes
Philippines	Yes	Yes (Hard copy also required)
Saudi Arabia	Yes	Yes
Singapore	Yes	Yes
South Africa	Yes	Yes
Spain	Yes	Yes
Switzerland	Yes	Yes
Taiwan	Yes	Yes
Thailand	Yes	Yes
UAE	Yes	Yes

Countries not included in this list do not require purchase orders or electronic invoicing

[1] List will be updated regularly and more locations will be added to electronic invoicing

JPMORGAN CHASE (JPMC)
CONTINGENT WORKER SINGLE POINT OF CONTACT TRAINING

Single Point of Contact's Roles and Responsibilities

Contingent Worker Onboarding Lifecycle

Types of Contingent Workers

Identity Request Form

Pre-Engagement Screening

Voltage Secure Mail

Resources

December 2018

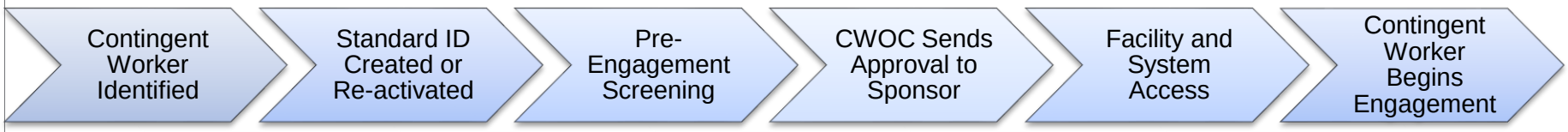
J.P.Morgan

Single Point of Contact's Roles and Responsibilities

A Single Point of Contact (SPOC) is an employee of the supplier who will submit all Contingent Worker information accurately and securely to the Contingent Worker Operation Center (CWOC). Suppliers can designate a maximum of eight people in their organization to serve as SPOCs. At least one SPOC must be designated prior to commencing any onboarding transactions. Responsibilities of the SPOC are outlined below:

- Serve as the main point of contact with the CWOC Group regarding the onboarding of Contingent Workers
- Ensure supplier personnel filter all requests to CWOC or other internal J.P. Morgan departments through the registered SPOC
- Works directly with the internal JPMC Assignment Sponsors to deliver a streamline onboarding process
- Initiates and ensures that Contingent Worker(s) complete Pre-Engagement Screening and meet assignment authorization requirements for the assignment location
- Follow-up, resolve, and serve as the main source of contact to deal with issues during Contingent Worker onboarding
- Know the distinction between *Provisional* versus *Confirmed* Standard IDs (SIDs)
  - *Provisional* SID – Status of the SID prior to clearing through the Pre-Engagement Screening
  - *Confirmed* SID – Status of the SID once the Pre-Engagement Screening is successfully completed and 'Cleared' status appears on the SPOCs End of Day Report

Contingent Worker Onboarding Lifecycle



Supplier works with Assignment Sponsor to identify Contingent Worker(s). Once identified Supplier SPOC determines if the Contingent Worker is a new or returning candidate.

Identity Request Form is sent to CWOC by the SPOC via Voltage Secure Mail. CWOC creates *Provisional* SID for Contingent Worker(s).

SPOC provides *Provisional* SID to the Contingent Worker(s) to initiate the Pre-Engagement Screening. Required screening components, depending on the region, are completed by the Contingent Worker.

Once the Contingent Worker(s) successfully clear through the Pre-Engagement Screening, the SID converts to a *Confirmed* status and CWOC notifies the Assignment Sponsor via Ready to Work Email.

Assignment Sponsor requests system and badge access, as needed.

Contingent Worker completes necessary training and begins their assignment.

Types of Contingent Workers

There are two types of Contingent Workers:

- New
- Returning

A Contingent Worker that already has an assigned SID due to a previous assignment or employment at JPMC, is considered a returning worker. Supplier SPOCs should identify returning workers and provide their previously assigned SID if known.

Prior JPMC employees (including JPMC legacy organizations) require a Human Resources re-entry check prior to the onboarding process to ensure that the individual is permitted to return to JPMC. The re-entry check is important in that it ensures that the individual was not removed for cause, or if the job was eliminated, that sufficient time has passed to return. For a former JPMC employee, the Supplier SPOC submits a Re-entry Check Form to the CWOC Group for the re-entry eligibility status. If the former employee is ‘eligible’, the SPOC may consider the individual as a candidate for an assignment.

When candidates (new, returning, or eligible former employees) have been selected for assignments, it is the responsibility of the Supplier SPOC to securely submit the required onboarding information via the Identity Request Form to the CWOC Group.

Identity Request Form

The Identity Request Form (IDRF) is used by the supplier SPOC to input the Contingent Worker's Information. It is the responsibility of the SPOC to submit the Identity Request Form in its entirety and as accurately as possible. While some of the JPMC related information is not available to the SPOC, it is one of the SPOC's duties to reach out to the Assignment Sponsor to gather the required information to submit on the form. The Legend tab provides an overview including who is responsible for completing each field, the Supplier or the Sponsor.

Once a secure email containing the IDRF has been submitted to CWOC, CWOC will review the submission for quality. Incomplete or inaccurate submissions will be rejected and the Supplier SPOC will be notified via email. Clean submissions will be processed and the Assignment Sponsor will receive an auto-generated email containing the Contingent Worker's *Provisional* SID. Supplier SPOCs will receive an End of Day Report each day with the SID results.

A *Provisional* SID permits the Assignment Sponsor to pre-order the following items to jumpstart the Contingent Worker's ability to begin their assignment once his/her SID switches to a *Confirmed* SID status.

- Workspace
- Phone
- Desktop Hardware (PC, Printer, VDI)

Pre-Engagement Screening

The SPOC initiates Pre-Engagement Screening (PES) by providing Contingent Worker(s) with their *Provisional* SID found on the End of Day Summary Report. It is the Contingent Worker's responsibility to follow the instructions for PES found in the Global Contingent Worker Pre-Engagement Screening (PES) Initiation Guide. Specific screening requirements and turn-around times will vary by country and are based on the Contingent Worker's physical work location. Each End of Day Summary Report will contain the Contingent Worker's PES results:

Screening Status	Description
Cleared	Worker has Cleared PES.
Not Cleared	Candidate is ineligible at this time. If you require further information regarding PES, the candidate can contact GWS.
Pending GS&I Review	Validation of PES record is required.
Rejected - Referral Related	Request was rejected. If you require further clarification, please contact CWOC.
SID Terminated - PES not Completed by Start Date	SID terminated because there is no record of cleared PES by the start date.

Contingent Workers may be privy to additional internal checks which are outlined within the "Pending Approval(s)" section and defined on the Legend tab of the EOD Summary Report. For more detailed information, please refer to the Contingent Worker Operations Center Onboarding Toolkit

The Assignment Sponsor will receive notification of the Contingent Worker's successful PES completion through a "Ready to Work" email which updates the Contingent Worker's SID status to *Confirmed*. Once the Ready to Work email is released, the Assignment Sponsor and Contingent Worker may begin to coordinate the Contingent Worker's assignment details (Logistics, Start Date, Time, etc.)

Voltage Secure Mail

Voltage SecureMail is a JPMC enterprise-wide solution for securing email communications with internal and external recipients

- SPOCs do not need any special software for incoming/outgoing secure messages.
- Both the message body and any attachments are always protected provided the recipient responds to the initial message received from CWOC.Group@jpmchase.com
- It will work with any fully functional browser on any platform.
- SPOCs need to create an account and test Voltage SecureMail during their initial setup with CWOC before they can successfully submit an IDRF with Contingent Worker information.

Resources

The majority of the forms needed for the onboarding process can be found on the JPMC internet on the Supplier Personnel Policies page. Forms housed on this page include:

- The Re-entry Check Form- This form is completed by Contingent Workers who have previously worked as an employee of JPMC or a JPMC heritage company.
- Identity Request Form- This form must be completed and submitted by the Supplier SPOC, with input from the Contingent Worker and the Assignment Sponsor, for each worker in order to obtain a JPMC *Provisional* SID and start the onboarding process.
- Global Contingent Worker Pre-Engagement Screening (PES) Initiation Guide - used by the Supplier and Contingent Worker to initiate the required regional background screening.
- Contingent Worker Operations Center Onboarding Toolkit – contains detailed information Assignment Sponsors and Suppliers need to onboard new and returning Contingent Workers to JPMC.

Contingent Worker Operations Center (CWOC)

- Email – CWOC.Group@jpmchase.com
- Helpline – (201) 595-1951 or (855) 900-2962

For all PES related inquiries please reach out to one of the Global Workforce Screening's regional teams:

- Europe / Middle East / Africa - EMEA.SECURITY.CHECKING@jpmorgan.com
- United States /Canada - gws.contingent.workers@chase.com
- Latin America / Bahamas - jpmc.latam.pes@jpmchase.com
- Asia Pacific - Asia.PES@jpmorgan.com

GOLD SUPPLIER PROGRAM

JPMorgan Chase & Co.

RISE TO THE OCCASION

"Innovative supplier engagement

is the hallmark of the Gold Supplier Program. Through it we hope to create shared, incremental value with our suppliers above and beyond the traditional supply chain goals of best price and best service. We partner with our Gold Suppliers in new ways with the goal of allowing suppliers to better reach their full potential with us, and helping JPMorgan Chase to become one of their best clients."

Ken Litton

Chief Procurement Officer, JPMorgan Chase & Co.

RISE TO THE OPPORTUNITY

JPMorgan Chase Gold Supplier status

is the firm's top designation for preferred suppliers. Suppliers may achieve Gold status by distinguishing themselves through excellent performance, integrity, and partnership with JPMorgan Chase to serve the needs of our clients, shareholders and employees.

The Gold Supplier Program

is a community encompassing suppliers large and small, public and private, diverse-owned businesses, and product categories of all types.

The program is designed to create strategic alignment and value by helping suppliers understand how to become more successful with JPMorgan Chase, and helping the firm to become the preferred customer in its supply markets.

Gold Suppliers are prioritized and recognized within JPMorgan Chase.

Gold Suppliers may receive:

- Facilitated opportunities for growth and category expansion, as appropriate;
- Enhanced insight to JPMorgan Chase's strategic agenda;
- Dedicated Gold Supplier Program relationship manager and communication channel;
- Simplified contracting, onboarding, and third party oversight processes;
- Faster invoice payment; or
- Special invitation to Gold Supplier events and networking

Becoming a Gold Supplier

is a milestone accomplishment in your relationship with JPMorgan Chase. The program is by invitation – you must be nominated by your Category Sourcing and Line of Business partner. Exemplary performance and partnership are critical to being nominated.

Gold Suppliers are measured against a series of program requirements for ongoing compliance. For more information, please visit **https://www.jpmorganchase.com/corporate/About-JPMC/GoldSuppliers.htm.**

GOLD SUPPLIER PROGRAM

"The Gold Supplier Program targets important partners who demonstrate a commitment to enabling our strategic agenda and ability to deliver to our clients, customers, and communities. It aims to define the way we do business together striving for a mutually beneficial relationship that helps to improve your competitive posture and working experience with JPMorgan Chase."

Laura Higgins

Head of Supplier Relationship Management,
JPMorgan Chase & Co.

JPMorgan Chase & Co.

Copyright 2018, JPMorgan Chase & Co. All rights reserved. Participation in JPMC's Gold Supplier Program does not alter any of the rights and obligations contained in existing agreements between suppliers and JPMC. JPMC reserves the right, in its sole discretion, to change, limit, modify or terminate the Gold Supplier Program, and to add suppliers to or remove suppliers from the Program at its discretion. Gold Suppliers are prohibited from disclosing their status as Gold Suppliers in any marketing or communication materials without the express written consent of JPMorgan Chase & Co's Global Media Relations department, to be granted or withheld in JPMC's absolute and sole discretion.

JPMorgan Chase & Co. Minimum Control Requirements

INTRODUCTION

These Minimum Control Requirements ("**Minimum Control Requirements**") are stated in a general manner, and JPMC recognizes that there may be multiple approaches to accomplish a particular Minimum Control Requirement. These Minimum Control Requirements are not intended to replace Supplier's standard policies and procedures but are intended to address the minimum controls that Supplier must have in place as part of Supplier's standard policies and procedures. As technology trends change, Supplier should ensure they are adhering to these Minimum Control Requirements as it relates to any new and emerging technologies. Supplier must document in reasonable detail how a particular control meets the stated Minimum Control Requirement. All Minimum Control Requirements apply to Supplier's subcontractors that have, process, or otherwise have access to JPMC Confidential Information or JPMC Systems. The term "should" in these Minimum Control Requirements means that Supplier will use commercially reasonable efforts to accomplish the stated Minimum Control Requirement. Any required policies, procedures, or processes mentioned in these Minimum Control Requirements must be documented, reviewed, and approved, with management oversight, on a periodic basis. Not all of the stated Minimum Control Requirements will apply to all Services or other Deliverables, but Supplier must be able to reasonably show how the Minimum Control Requirement does not apply. These Minimum Control Requirements do not limit Supplier's obligations under the Agreement or applicable Law, and do not limit the scope of an audit by JPMC. Supplier must comply with and have processes for researching, evaluating, and complying with, all Laws in the applicable jurisdiction(s).

As used in these Minimum Control Requirements, any capitalized terms not defined herein shall have the same meaning as set forth in the Master Agreement relating to the Services and other Deliverables to which these Minimum Control Requirements relate.

TECHNOLOGY GOVERNANCE, RISK, AND COMPLIANCE

- The effectiveness of controls must be regularly validated through a documented risk assessment program and appropriately managed remediation efforts.
- A risk assessment must be performed annually to verify the implementation of controls that protect business operations and JPMC Confidential Information.
- A documented set of security policies and procedures must govern the receipt, transmission, processing, storage, control, distribution, retrieval, access, presentation, and protection of information, assets, and associated services.
- A risk-based exception management process must be in place for prioritization and remediation or risk acceptance of controls that have not been adopted or implemented.
- Security policies and responsibilities, including cybersecurity awareness training, must be communicated and socialized within the organization to Supplier Personnel.

PHYSICAL AND ENVIRONMENTAL SECURITY

- Physical and environmental security processes and procedures must be in place for facilities with access to, or storage of, JPMC Confidential Information.
- Personnel should be granted access to areas of the facility based on the principle of least privilege.
- Physical access to facilities must be restricted, with all access recertified on a regular schedule.
- Detective monitoring controls (e.g., CCTV) must be in place with a defined retention period.
- Facilities must maintain appropriate environmental controls, including fire detection and suppression, climate control and monitoring, power and back-up power solutions, and water

damage detection.
- Environmental control components must be monitored and periodically tested.

DATA PROTECTION

- Suppliers and dependent subcontractors must have sufficient information classification for the purpose of data protection
- JPMC Highly Confidential and Confidential Information must be protected and encrypted in transit and at rest (including in backup) as well as when shared with Supplier's subcontractors.
- All authentication credentials (e.g., passwords, personal identification numbers, challenge answers) must be encrypted in transit and at rest.
- Supplier's data protection policy must cover encryption, key and certificate lifecycle management, permitted cryptographic algorithms and associated key lengths, message authentication, hash functions, digital signatures, and random number generation.
- Data protection policy must be reviewed against industry standards on a regular basis.
- Supplier must implement appropriate technical configuration for the protection of encrypted portable media.
- Procedures around cookie management must be compliant with applicable laws and regulations.

IDENTITY AND ACCESS MANAGEMENT

- Documented logical access policies and procedures must support role-based, "need-to-know" access based on the principle of least privilege, and ensure segregation of duties during the approval and provisioning process.
- Logical access policies must cover remote access, access request approval prior to access provisioning and periodic recertification of access.
- Each account provisioned must be uniquely identified.
- A privileged account management process and control policy must be documented, covering privileged (system or elevated user) and non-privileged (personal) account separation, privileged account discovery, safeguarding of privileged accounts, post activity usage review requirements, and assurance that non-interactive privileged accounts (e.g., system accounts) are not used interactively by end users
- A documented authentication and authorization policy must cover all applicable systems and networks and include password provisioning requirements, password complexity requirements, password resets, thresholds for lockout attempts, thresholds for inactivity, and assurance that no shared accounts are utilized.
- The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change of role.
- Multi-factor authentication must be implemented for:
    - The initiation of any interactive privileged access session.
    - External connectivity to the JPMC network.
    - Applications directly accessible from the internet.
    - The administration of application access.
- Federated identity management must be implemented for JPMC access to Supplier systems via industry standard security assertion markup language (SAML).

SECURITY CONFIGURATION

- Supplier must implement controls over its communication network to safeguard data.
- A network diagram, to include all devices, as well as a data flow diagram must be kept current.
- Network devices must have internal clocks synchronized to reliable time sources.
- Standard security configurations, using the principles of least functionality/privileges, must be

established and security hardening demonstrated.

- Information systems must be deployed with appropriate security configurations and reviewed periodically for compliance with Supplier's security policies and standards.
- Drift or deviation from hardened builds/security configuration baselines must be identified, reported, and remediated.
- Malware protection mechanisms must exist to detect and/or prevent against malware and other threats.
- Malware protection mechanisms must be configured to perform real-time or scheduled scans of systems, and alert when malware is discovered.
- All devices and malware protection mechanisms must be kept up-to-date with latest anti-virus software and definitions.
- Network and host-based intrusion detection and/or intrusion prevention systems must be deployed with generated events fed into centralized systems for analysis.
- Supplier must have policies, procedures, and controls that ensure proper control of an electronic mail and/or instant messaging system that displays and/or contains JPMC information.
- Preventive controls must block malicious messages and attachments as well as prevent auto-forwarding of emails.

SECURITY OPERATIONS

- Supplier Personnel must be trained to identify and report suspected security weaknesses, suspicious activity, and security events or incidents.
- Data loss prevention (DLP) technology, processes, and/or solutions must be deployed to protect against the exfiltration of JPMC information.
- Supplier must have a security event/incident response policy and procedure.
- Retention schedule for various logs must be defined and followed.
- Security event logs from information systems must be collected, centrally managed, analyzed, and correlated for the purpose of detecting anomalous behavior that may indicate malicious events/incidents.
- A fraud and threat detection, prevention and mitigation program, processes and procedures for monitoring and reporting actual and suspected instances of fraud, and specific notification and communication, internally and to JPMC, must be established.
- Supplier should have a procedure for conducting digital forensics including data collection, data/evidence preservation for future analysis, analysis, reporting of findings, and closure.
- A process should be in place to conduct attack simulations including social engineering exercises (e.g., phishing), red teaming, and tabletop exercises with appropriate reporting, remediation/acceptance, and tracking of findings.
- Access to non-corporate/personal email and instant messaging solutions must be restricted.

VULNERABILITYMANAGEMENT

- Supplier must include as part of their vulnerability management program, the receipt of vulnerability related security alerts and intelligence from external and internal sources in order to identify and monitor for vulnerabilities in their environment.
- Vulnerability scans (authenticated and unauthenticated) and penetration tests must be performed against internal and external networks and applications periodically and prior to system provisioning for all systems that process, store, or transmit JPMC Confidential Information.
- Any critical vulnerabilities identified through intelligence gathering, vulnerability scans, or penetration testing must be prioritized and remediated within a well-defined timeframe commensurate with the vulnerability risk.

PRIVACY

- Supplier must implement effective controls to ensure appropriate processing and protection of

Personal Information.

- Social Security Numbers or other national identifiers must not be utilized as User IDs for logon to applications.
- Privacy impact assessment must be conducted during the requirements phase of system development to evaluate the impact to Personal Information and review the scope of monitoring.
- The privacy impact assessment must not conflict with any applicable local and other Laws.
- Supplier must have procedures for obtaining consent from users to collect Personal Information, giving users the ability to access, correct, opt-out, delete, restrict, make portable, or object to the processing of Personal Information.
- A privacy notice or information banner must be in place, requiring acknowledgement by the end user whenever Personal Information is collected, transmitted, processed, or stored.
- Procedures around collecting Personal Information as required by the Law must be defined and restrictions on disclosing that Information must be documented.
- Supplier must have a process to notify JPMC of any event that may or will impact that confidentiality, integrity or availability of personal information, including unauthorized or suspicious intrusion into systems storing such personal information.

TECHNOLOGY DEVELOPMENT

System Development Life Cycle (SDLC)

- Suppliers must operate an established System Development Life Cycle (SDLC) process.
- SDLC governance must be established, documented, and enforced to identify and remediate defects, vulnerabilities, coding errors, and design flaws prior to production using a risk-based approach.
- The SDLC must establish the control requirements for software development that are applicable to any software and development framework or model used.
- The SDLC must include a Secure Design Review, and preventive and detective controls in line with industry standards (such as OWASP) to identify vulnerabilities and design flaws.
- Functional and non-functional requirements must be continuously identified and implemented to prevent software from becoming obsolete.

Third-Party Software

- Third party and open source code or software used must be appropriately licensed, inventoried, and where commercially licensed, be fully supported by the vendor.

TECHNOLOGY OPERATIONS

- Documented operational procedures must ensure correct and secure operation of assets.
- Operational procedures must include monitoring of capacity and performance.
- Changes to the production system, network, applications, data files structures, other system components and physical/environmental changes must be monitored and controlled through a formal, documented change control process.
- Changes must be tested prior to implementation and reviewed for impact.
- Changes must be approved prior to implementation, and evaluated after implementation to ensure that the expected outcome was achieved.
- An emergency change management procedure must documented.
- Any changes materially affecting JPMC services must be communicated to JPMC prior to implementation.
- Infrastructure assets must follow a documented and approved technology maintenance process.

THIRD PARTY RELATIONSHIPS

- Supplier's subcontractors must be identified, assessed, managed, and monitored in accordance

with the terms of the Master Agreement with JPMC, including compliance with JPMC's Minimum Control Requirements and Supplier Code of Conduct applicable to any such services.

DATA RISK MANAGEMENT

- Suppliers and dependent subcontractors that regularly provide data to JPMC must maintain and provide a data dictionary or equivalent data classification artifact, including any agreed-upon metadata for data provided to JPMC.
- Supplier and dependent subcontractors must have controls in place to allow JPMC to validate that a complete set of data has been received in an agreed-upon format. Supplier must have a process for notifying JPMC of errors for data transmitted to or from JPMC in accordance with quality specifications for the accuracy, timeliness, and completeness of the data.
- All JPMC data provided to and stored by Supplier and dependent subcontractors must be stored and retained in a manner that:
    - includes the capability to access and retrieve the data as needed.
    - avoids loss due to media decay or technology obsolescence.
    - provides reasonable safeguards against ordinary hazards, man-made hazards, and disasters.
    - is in accordance with applicable laws, regulations, and contractual obligations.
    - protects the data from unauthorized access/alteration.
- If Supplier or dependent subcontractor hosts data on behalf of JPMC, Supplier and dependent subcontractors must maintain and validate with JPMC (at least annually) a complete and accurate inventory of JPMC data with the following attributes:
    - Classification
    - Retention/Destruction Requirements (and execution of those requirements)
    - Location
- Suppliers and dependent subcontractors who receive, provide, transmit, store, create, generate, collect, control, process, or have access to JPMC Confidential Information must do so solely to provide services to JPMC.
- Supplier and dependent subcontractors must be able to maintain data provenance.

TECHNOLOGY ASSET MANAGEMENT

- Supplier must have a sufficient technology asset registration policy and procedure, including unique identifiers for all assets, appropriate classification, asset ownership, and asset location, including proper licensing and meeting all legal, regulatory, contractual, or support requirements.
- Supplier must maintain an appropriate technology asset inventory governance structure to include recorded changes to asset records, sufficient back up of asset registers, annual integrity validation of the asset registers, asset ownership recertification, timely asset register updates when asset records are altered, regular license audits of assets, procedures addressing lost/stolen assets, and remediation of unauthorized assets.
- A technology asset lifecycle management program must be put in place that includes accurate lifecycle status of all assets, identification of assets not in compliance with the lifecycle management policy, and notification to asset owners of non-compliant assets.
- A technology asset provisioning and disposal program must be in place to include only procuring technology assets from appropriately sourced suppliers and disposing of/removing/deleting all technology assets in a secure manner when they reach end of life.
- Supplier must ensure assets are transported in a secure manner.

INCIDENT AND EVENT MANAGEMENT

- Documented incident, event, or problem management procedures must include systematic tracking from discovery to resolution.

- Supplier's event management policy and procedures must account for the detection, analysis, and presentation of anomalous events that indicate deviation from the norm beyond a defined threshold and engage JPMC via an incident management process.
- Supplier's incident management policy and procedures must also include prioritization, roles and responsibilities, internal escalation, notification to JPMC, tracking and reporting, containment and remediation, and preservation of data to maintain forensic integrity.
- Supplier's problem management policy must include documenting root cause analysis, implementation of permanent fix, preventative actions, and service improvement opportunities, providing conclusions to JPMC.

BUSINESS RESILIENCY

- Supplier must have formal, comprehensive business resiliency plans to enable timely, orderly, and sustainable recovery of business, support processes, operations and technology elements associated with the services provided for JPMC.
- Supplier must perform a Business Impact Analysis (BIA) to determine their business resilience process criticality and to define a Recovery Time Objective (RTO) for all processes they utilize to support the services or functions being performed for JPMC.
- Business resiliency plans must identify key resources and address business interruptions of those resources supporting all JPMC services, including those provided by Supplier's subcontractors
- Supplier recovery plans must have recovery strategies in place to adequately address the following disruption scenarios to meet JPMC RTO and service level expectations (as defined in the relevant contracts):
    - Loss of staff
    - Loss of site
    - Loss of application (where application disaster recovery is available)
    - Loss of Supplier's subcontractors (where subcontractor recovery is available)
- The resiliency plans must have acceptable alternative work locations/strategies in place to ensure service level commitments are met.
- Supplier recovery plans must be updated, reviewed and approved at least annually or as material changes occur within Supplier's operating environment.
- Resiliency plans must be tested on a regular basis, noted deficiencies/failures should be addressed timely, and testing should:
    - be conducted in conditions comparable to production
    - demonstrate recovery within the established Recovery Time Objectives
    - be tested annually
- Any change that could affect the recovery of the process or infrastructure, may involve, but is not limited to, changes in Supplier's business strategy, service, process, assets, and regulatory/legal obligations, resulting in significant changes to the BIA or plans must require a new test of the recovery plans affected by the significant change.

TECHNOLOGY RESILIENCY

- Supplier must have formal technology recovery plans to identify the resources and specify actions required to help minimize losses in the event of a disruption to services provided to JPMC or resources supporting those services.
- Supplier recovery plans must identify Supplier's own critical processes, supporting assets, dependencies, critical points of failure, recovery staff personnel and recovery capabilities to address business interruptions to processes that support JPMC services.
- Supplier must have formal technology recovery plans and technical capability to limit service interruption and recover from a destructive cyber event where both the primary (production) and secondary (disaster recovery) systems or data have been compromised or destroyed.
- Plans must include how to redeploy an application and restore associated data following a loss.

- Recovery plans must also include Supplier's subcontractors, including cloud service providers.
- Recovery plans must be tested on a regular basis using sufficient methodologies and frequencies which include testing long term strategies. Test failures must be re-tested within a reasonable amount of time.
- Applications and associated hosts must employ a backup policy in order to meet full application recoverability. The policy must define datasets, frequencies, criteria for a successful backup, annual test requirements, offsite storage requirements, and retention periods. The backup policy must be annually reviewed and recertified.
- Processes and procedures must be in place to enable recovery of internal IT services to normal production operation, within the RTO, as defined in relevant contracts, in the event of planned and/or unplanned loss of application deployment or loss of site.
- Any change that could affect the recovery of the process or infrastructure, including significant changes in personnel, organizational structure, technology, location, or strategy must require a new test of the technology recovery plans affected by the significant change.
- Supplier must have a crisis management framework including initial notification to JPMC, ongoing contact with JPMC during an incident impacting the services being performed by Supplier, and an after action review of the incident.
- JPMC Confidential Information must be available upon request, in an industry standard format, so as to ensure portability and interoperability.

ORGANIZATIONAL SECURITY

- Supplier personnel assigned to JPMC Services must review the JPMC Supplier Code of Conduct available at: https://www.jpmorganchase.com/about/suppliers.
- Supplier personnel must notify JPMC in the event of any potential or actual conflicts of interest between Supplier personnel's outside business activities and personal relationships and JPMC business, clients, or employees.
- Supplier must provide training to Supplier Personnel on job responsibilities, including cybersecurity awareness, and ensure Supplier personnel complete any assigned JPMC training.
- Supplier must conduct a formal, tracked performance and appraisal review process of its personnel.
- Supplier must maintain current organizational charts representing key management responsibilities for services provided to JPMC, including all related services provided by dependent third party suppliers.
- Supplier must perform appropriate background checks on its personnel.
- Supplier must ensure its personnel have agreed to non-disclosure or confidentiality obligations before assigning to JPMC services and giving access to JPMC systems and information.

CUSTOMER CONTACT

- If it is providing customer service (e.g., customer contact agents and related operations), Supplier must have defined and enforced operational procedures that ensure the confidentiality, integrity and availability of JPMC Confidential Information, as well as the provision of services and other deliverables in compliance with the relevant contract(s).
- Supplier must maintain and implement effective procedures for the authentication of each customer, including as may be directed by JPMC.
- Customer contact agents must receive privacy training (addressing, e.g., proper handling of individual personal information in light of privacy laws and regulations), including as may be specified in the relevant contract(s) and/or as directed by JPMC.
- Any complaints received regarding JPMC or any services provided for or on behalf of JPMC, must be reported to JPMC as may be specified in the relevant contract(s) and/or as directed by JPMC.

JPMorgan Chase & Co. Diversity, Equity, and Inclusion Standards

INTRODUCTION

JPMorgan Chase is dedicated to the development and support of diverse communities from historically underrepresented groups including minorities, women, military veterans, people with disabilities, and members of the LGBTQ+ community. To ensure our Suppliers share the same commitment to diverse communities, the following Diversity, Equity, and Inclusion Standards have been developed for our Suppliers. With JPMC Suppliers adhering to similar principles of Diversity, Equity, and Inclusion, we can best serve our consumer base.

These Diversity, Equity, and Inclusion Standards are stated in a general manner, and JPMC recognizes that there may be multiple approaches to achieve a particular Diversity, Equity, and Inclusion Standard. These Diversity, Equity, and Inclusion Standards are not intended to replace Supplier's standard policies and procedures but are intended to address the minimum standards that the Supplier must have in place as part of Supplier's Diversity, Equity, and Inclusion program. Upon request, Supplier must document in reasonable detail how Supplier meets a particular Diversity, Equity, and Inclusion Standard. Supplier's Diversity, Equity, and Inclusion Standards must be documented, reviewed, and approved, with management oversight, on a periodic basis. These Diversity, Equity, and Inclusion Standards do not limit Supplier's obligations under the Agreement or applicable Law, Supplier must comply with and have processes for researching, evaluating, and complying with, all Laws in the applicable jurisdiction(s).

DIVERSITY, EQUITY, AND INCLUSION STANDARDS

- A documented Diversity, Equity, and Inclusion program must be in place that should include (but shouldnot be limited to) appropriate hiring practices, anti-discrimination, reporting/escalation, and anti-retaliation.
- All new-hire and existing supplier personnel must be subject to training on Supplier's Diversity, Equity, and Inclusion program with appropriate tracking of training completion.
- Supplier must track its workforce diversity across the enterprise, including rates of attrition and promotion amongst diverse employees.
- Supplier must have appropriate procedures for receiving complaints of discrimination, investigating those complaints, and escalation of complaints as needed.
- Supplier must have a third party Diversity, Equity, and Inclusion program in place to monitor their own third parties' DE&I commitment.

Global Technology Acceptable Use Policy for Contingent Workers (AUP-CW)

The Acceptable Use Policy for Contingent Workers (AUP-CW) defines appropriate and inappropriate uses of JPMorgan Chase technology or information resources irrespective of their medium, and provides guidance to contingent workers' use of these resources, whether those resources are used for personal or business purposes.

For each new engagement in which a JPMC contingent worker is assigned, all JPMC contingent workers are required to confirm that they understand their information security responsibilities by reviewing and affirming to this AUP-CW and the Supplier Code of Conduct.

DEFINITION

For the purposes of this document, the terms "inappropriate use" of JPMorgan Chase information resources and "inappropriate material" include any uses or material that could be construed by a reasonable person or a court of law as being generally offensive, abusive, illegal, immoral, or unethical; in violation of applicable laws, regulations, or corporate policies or standards; or that in any way jeopardizes the confidentiality, integrity, or availability of the Firm's technology or information resources or intellectual property, or that compromises the Firm's tangible or intangible assets, including its name, reputation, and logo. Contingent workers must not use the Firm's technology or information resources for inappropriate purposes. Inappropriate use is grounds for termination of engagement and other remedies available to JPMC.

As it relates to contingent workers, an "Assignment Sponsor" is the day-to-day manager for the contingent worker who is responsible for the engagement.

APPROPRIATE USES

The following list is provided as guidance to contingent workers; it is not meant to include examples of all types of appropriate use:

- Agree to report to your Assignment Sponsor any possible threat or incident to ensure the Firm's information resources in their area are protected from accidents, tampering, viruses and unauthorized use or modification.
- Understand that the Firm has a vested interest in maintaining the integrity of copyrighted information, and should be particularly sensitive to copyrighted information.
- Agree to handle all information stored on a computer or downloaded to portable media such as flash drives and hard copies with appropriate care to prevent unauthorized disclosure of the information.
- Agree to protect passwords and never disclose or share them with anyone, and agree to make passwords hard to guess by following the Firm's password composition standards.
- Agree to report to their Assignment Sponsor any possible or actual security violations that come to their attention, and understand that violation of this AUP-CW can lead to termination of engagement.
- Understand that by using JPMorgan Chase's information resources, contingent workers knowingly agree and consent to their usage being monitored and examined, and acknowledge JPMorgan Chase's right, subject to applicable laws and regulations, to conduct such monitoring, including, but not limited to, retrieving, reading, inspecting and disclosing any information therein.

INAPPROPRIATE USES

The following list is provided as guidance to users; it is not meant to include examples of all types of inappropriate use. If you are unsure if an anticipated use of JPMorgan Chase information resources is inappropriate, consult with your manager or your LOB Information Risk Manager.

1. **General Terms** – Inappropriate use of JPMorgan Chase's information resources includes, but is not limited to, the following:

    - Using information resources for personal business.
    - Using information resources for actions that violate this AUP-CW, the Supplier Code of Conduct or any other JPMorgan Chase supplier policy.

- Using information resources in a manner that jeopardizes the confidentiality, integrity, or availability of the information resources.
- Transmitting information in violation of applicable law or regulation, this AUP-CW, the Supplier Code of Conduct, or any other JPMorgan Chase supplier policy.
- Using non-JPMorgan Chase owned, leased, or authorized equipment including removable storage media to store, process, or transmit non-public JPMorgan Chase information.

2. **Inappropriate Uses of Email** - Inappropriate use of email includes, but is not limited to, the following:

    - Sending or forwarding email from a JPMorgan Chase managed email account to:
        - A personal account or external corporate account. Contingent workers must not forward emails from a JPMorgan Chase managed email account to their personal email account or external corporate email account for any purpose.
        - Any non-JPMorgan Chase managed email account via directory entries, agents, or applications, including those that are automated.
    - Using a non-Firm managed account to store JPMorgan Chase email.
    - Forwarding electronic chain letters.
    - Using a JPMorgan Chase managed email account for unauthorized solicitation purposes.
    - Using a JPMorgan Chase managed email account for any other purpose outside the scope of engagement.

3. **Inappropriate Uses of Authentication Information** – Users must establish, alter, and retain sole, secure knowledge of passwords and any other means of identity authentication as directed by JPMC. Inappropriate uses/conditions that could compromise authentication information, systems, or network security include, but are not limited to, the following:

    - Using software to log keystrokes in a production environment.
    - Using or possessing password cracking programs, security vulnerability assessment, exploitation tools, or network sniffers to capture and view transmitted data, network discovery tools, system discovery or inventorying tools, unless as part of engagement as expressly authorized in a contract with JPMC and signed by both JPMC and Supplier.

4. **Inappropriate Uses of Software** – Inappropriate activity with software files/programs includes, but is not limited to, the following:

    - Downloading, uploading, copying, or distributing software or electronic files in violation of their copyright.
    - Downloading, uploading, saving, or trading music or video files whether or not the action is in violation of applicable copyright restrictions.
    - Downloading or uploading any software or electronic files, including legitimate information, without up-to-date virus protection measures in place.
    - Intentionally accessing, downloading, uploading, saving, or sending sexual, pornographic, discriminatory, or criminal material.

5. **Inappropriate Activity Regarding System Builds/Configurations** – Inappropriate activity to modify system builds or configurations includes, but is not limited to, the following:

    - Disabling or removing any security software; for example, access control or computer virus control.
    - Installing, disabling, or removing software, other than device drivers, on a JPMorgan Chase computer.

6. **Inappropriate Internet-related Activity** – Inappropriate Internet-related activity includes, but is not limited to, the following:

    - Sending or storing the Firm's data or files on non-JPMC web-based data storage services, for example, Google Drive, Mega, 4Shared, iCloud, etc.
    - Establishing undocumented and unapproved Internet or other external network connections that could allow a non-JPMorgan Chase user to gain access to JPMorgan Chase systems and

information.

- Using the JPMorgan Chase Intranet to access non-corporate-standard email accounts such as MS Hotmail, Yahoo Mail, and Gmail.
- Placing JPMorgan Chase material (software, internal memos, etc.) on any publicly accessible Internet computer that supports anonymous file transfer protocol (FTP).
- Posting non-public JPMorgan Chase or any other type of information that may compromise the security of the Firm's assets or violate supplier policies or the Supplier Code of Conduct via Internet-accessible message boards, blogs, social networks and other forms of communication. For more details, please also see the Continent Work Social Media Policy.
- Using the JPMorgan Chase name or logo on the Internet.
- Gambling.
- Accessing or downloading pornographic material.
- Making or posting indecent, offensive, discriminatory, harassing, or disruptive remarks, or other inappropriate content.
- Creating or using intranet blogs that contain Confidential or Highly Confidential information.

Doing business securely in the financial services industry

JPMorgan Chase Summary of Guidance from the U.S. Treasury and industry regarding key security and risk management practices for new suppliers seeking to serve financial services industry

February 2019

The information in this document is general in nature and originates from 3rd party sources. The information is shared on an “as-is” basis without any type of promise or representation as to its quality or usability.

© 2019 JPMorgan Chase & Co. All rights reserved.

Preface

The financial sector is a critical part of the U.S. economy. Advancing the **safety, soundness, and resiliency of the financial sector** by mitigating and protecting it from risks is a **shared goal** for all financial sector participants as well as financial services regulatory community.

Companies that seek to do business in the financial sector as **suppliers are required to perform all their activities in a safe and sound manner and in compliance with applicable laws.** This is especially important when a supplier service involves access to confidential data or delivery of critical service.

Currently there are numerous regulatory and industry sources that specify such requirements. New suppliers are finding it difficult to comprehend and comply. This situation creates a barrier to entry that could stifle innovation and reduce competitiveness.

The U.S. Treasury Guidance helps to consolidate existing requirements into a **clear, concise set of nationwide best practices that new suppliers seeking to serve financial sector should adopt and be ready to demonstrate.**

- The Guidance was developed in early 2018 by the U.S. Treasury and representatives of several U.S. financial institutions.
- The Guidance is organized around the five categories of the NIST Cybersecurity Framework[1], with "Engage" category added to cover requirements beyond cybersecurity (for example, financial stability requirement for new suppliers).

The U.S. Treasury encourages all companies that are positioning themselves to become suppliers to the financial sector to consider and adopt this Guidance. This will enable such companies to effectively engage with financial institutions, and also elevate the security of new suppliers' operations–thus helping to keep our industry and our country safe.

1 National institute of Standards and Technology Cybersecurity Framework (NIST CSF) is the de facto standard for firms seeking guidance to counter cyber threats according to U.S. Department of the Treasury, Office of Financial Research, "Financial Stability Report" of 15th December 2017. Federal entities and Sector-specific agencies (SSA) are promoting and supporting the adoption of the NIST CFA in all critical infrastructure sectors (including financial sector).

Key security and risk management practices for new suppliers seeking to serve financial services industry

Identify

1. Supplier should **identify, classify and manage all assets**–data, systems, software, devices, personnel, facilities, any other–that it uses to provide services to financial institutions.
2. Supplier should establish a **risk management program** to proactively identify, assess and mitigate risks to all assets that it uses to provide services to financial institutions.
3. Supplier should establish a **third party risk management program** to proactively manage risks associated with their third parties and subcontractors.
4. Supplier should establish policies, procedures, controls to ensure **compliance** with all applicable legal, regulatory, risk, security and operational requirements.

Protect

5. Supplier should implement **perimeter and network security** controls to permit only approved and authorized communications between network domains.
6. Supplier should **limit access** to data, systems, software, devices, personnel, facilities and other to only authorized users to perform authorized activities.
7. Supplier should **encrypt data** while in transit and at rest and have implement adequate measures to manage and protect cryptographic keys.
8. Supplier should **protect data throughout data lifecycle** (from creation through disposal), consistent with supplier's risk management strategy.
9. Supplier should ensure that all systems are **configured securely,** and review security configurations on a regular basis.
10. Supplier that develops software should implement **secure software development practices.**
11. Supplier should have strict **change management** procedures that require documentation, review and approval of all changes to production environment.
12. Supplier should provide regular **training and communications** on security policies and risks such as social engineering, phishing and other.
13. Supplier should have **standard contract terms** for their third parties. The terms should include all relevant legal protections.

Key security and risk management practices for new suppliers seeking to serve financial services industry (cont'd)

Detect

14. Supplier should continuously gather and analyze information on new and existing **threats and vulnerabilities.**
15. Supplier should enable logs of key systems and user activities, and on a regular basis **aggregate and analyze logs** to identify any unauthorized activity.
16. Supplier should periodically **scan internal and external networks and applications** for vulnerabilities.
17. Supplier should implement **Data Loss Prevention** mechanisms to limit unauthorized or unintentional exfiltration of data.
18. Supplier should implement a **background check** process for its employees and contractors.

Respond

19. Supplier should have an **incident response** plan. Staff should be trained to execute the plan and execution should be tested periodically. Incident response plan should include notification to affected financial institutions.
20. Supplier should implement a strict **patch management** process to identify and classify vulnerabilities, and implement patches within a defined and reasonable timeframe.

Recover

21. Supplier should maintain **business continuity and disaster recovery** plans that define resources and actions to help minimize losses in the event of a disruption to the business unit, application, or infrastructure.
22. Supplier should periodically **backup data** in a secure manner and verify recoverability of data and software.

Engage

23. Supplier should be able to provide audited financial statements to demonstrate their **financial stability** to financial institutions they are looking to engage with.
24. Supplier should **support assessments of its controls** by the financial institutions and assessment firms. This includes providing the required controls documentation, as well as allowing assessors to inspect and test controls.

CONTROLLER - TO - PROCESSOR SCCs

PART 1

STANDARD CONTRACTUAL CLAUSES

SECTION I - INITIAL PROVISIONS

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'); and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: "**Clauses**").

(c) these Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) the Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause – deleted.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "**personal data breach**"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "**sensitive data**"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "**onward transfer**") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) SPECIFIC PRIOR AUTHORISATION. The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least 180 days prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination – including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as

possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 **Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the EU Member State in which the data exporter is established.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

The following Annexes form part of the Clauses, must be completed where applicable, and must be signed by the parties where indicated.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Name: JPMorgan Chase Bank, N.A.

Address: 383 Madison Avenue, New York, New York 10179, United States

Contact person's name, position and contact details: As specified in the Agreement.

Activities relevant to the data transferred under these Clauses: As specified in the Agreement.

Signature and date:The parties agree that execution of the Agreement by the data importer and the data exporter shall constitute execution of these Clauses by both parties as follows: (a) on 27 October 2021, where the effective date of the Agreement is on or before 27 September 2021, or (b) otherwise, on the effective date of the Agreement.

Role: Controller

2. **Data importer(s)**:

Name: As specified in the Agreement.

Address: As specified in the Agreement.

Contact person's name, position and contact details: As specified in the Agreement.

Activities relevant to the data transferred under these Clauses: In accordance with the Deliverables provided under the Agreement.

Signature and date: The parties agree that execution of the Agreement by the data importer and the data exporter shall constitute execution of these Clauses by both parties as follows: (a) on 27 October 2021, where the effective date of the Agreement is on or before 27 September 2021, or (b) otherwise, on the effective date of the Agreement.

Role: Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Concern current / former/ prospective employees; current / former / prospective wholesale clients; current / former / prospective retail clients; visitors to websites / online services, or as otherwise described in the Agreement.

Categories of personal data transferred

Personal Data including data relating to data subjects provided to the Supplier in connection with the Deliverables by or at the direction of JPMC, or as otherwise described in the Agreement.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The frequency of the transfer shall be as described in the Agreement.

The nature of the processing shall be as described in the Agreement.

The purpose(s) of the data transfer and further processing shall be as described in the Agreement.

The period for which the personal data will be retained, or the criteria used to determine that period shall be as described in the Agreement.

To the extent permitted, transfers to sub-processors shall be conducted in accordance with the terms of the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

The Supervisory Authority of Hesse, Germany

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Importer shall comply with the measures set out in JPMC's security policies in force from time to time, including JPMC's Minimum Control Requirements, a current copy of which is located at:

https://www.jpmorganchase.com/about/suppliers/guidelines-documents

or as otherwise specified in the Agreement.

ANNEX III

LIST OF SUB-PROCESSORS

The data exporter has not authorised the use of sub-processors unless otherwise agreed or as set forth in the Agreement.

Covered Jurisdiction ex-UK – ADDENDUM

Where:

A. the entity exporting data is an entity not established in any Member State of the European Union (excluding the UK);

B. the entity exporting data is subject to the law of the country in which it is established ("**Applicable Law**"); and

C. JPMorgan Chase Bank, N.A. and data importer have entered into the Standard Contractual Clauses in respect of the transfer of personal data from the entity exporting data to the data importer as more particularly described in Annex I to the Standard Contractual Clauses, the parties hereby agree as follows:

1.1 the terms of the Standard Contractual Clauses are amended as follows:

(a) the terms "personal data", "special categories of data", "process/processing", "controller", "processor", "data subject", "supervisory authority", "Data Protection Authority", "automated decision", "personal data breach" and "third country" shall be interpreted in accordance with their equivalent terms in Applicable Law;

(b) all references to the term "**Member State**" shall be deleted and replaced with "**country**";

(c) all references to "**Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)**", including references to "**Regulation (EU) 2016/679**", "**GDPR**" and/or any references to the articles of Regulation (EU) 2016/679 shall be deleted and replaced with "**Applicable Law**" or the "relevant principles consistent with Applicable Law" where Applicable Law does not expressly provide for the indicated ; and

1.2 the parties shall comply with the provisions of Applicable Law at all times in relation to the transfers contemplated under the Standard Contractual Clauses as more particularly described in Annex I; and

1.3 in the event that there is any conflict between Applicable Law and the Standard Contractual Clauses, Applicable Law shall govern;

1.4 rights and obligations provided in the Standard Contractual Clauses shall apply only to the extent provided for under Applicable Law; and

1.5 Clause 17 shall read "These Clauses shall be governed by the law of the country in which the data exporter is established.". The remainder of Clause 17 shall be deleted; and

1.6 for purposes of Annex IC, the competent supervisory authority shall be the supervisory authority of the country in which the data exporter is established.

Covered Jurisdiction – UK ADDENDUM

UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers of data from the UK subject to the UK GDPR. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract. The following Addendum forms part of the Addendum EU SCCs.

Part 1: Tables

Table 1: Parties

Start date	Data importer and data exporter shall be deemed to have executed these Clauses effective of the following date: (a) on 27 October 2021, where the effective date of the Agreement is on or before 27 September 2021, or (b) otherwise, on the effective date of the Agreement.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	As indicated in Annex I.A	As indicated in Annex I.A
Key Contact	As indicated in Annex I.A	As indicated in Annex I.A
Signature (if required for the purposes of Section 2)	Not required.	Not required.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: As above. Reference (if any): N/A Other identifier (if any): N/A

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: As above.
Annex 1B: Description of Transfer: As above.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As above.
Annex III: List of Sub processors (Modules 2 and 3 only): N/A

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☒ Exporter ☐ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.

Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

> "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

c. Clause 6 (Description of the transfer(s)) is replaced with:

> "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

> "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

> "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

> "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

> "These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

> "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a its direct costs of performing its obligations under the Addendum; and/or

    b its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

JPMorgan Chase Bank N.A. Supplier Travel and Expense Policy

The JPMorgan Chase Bank N.A. Supplier Travel and Expense Policy ("Policy") applies to a supplier of products or services ("Supplier") to JPMorgan Chase Bank, National Association ("JPMC"), or a JPMC affiliate(s). For purposes of this Policy, "Supplier Personnel" will include Supplier's employees, temporary employees, independent contractors, subcontractors, agents or any other person or entity acting on its behalf.

a) JPMC and Supplier agree that all budgets, approvals and other relevant information relating to any travel and expenses incurred in order to provide products or services on behalf of JPMC must be mutually discussed, pre-approved and documented in a written instrument and signed by both parties in advance. Unless specifically authorized in writing by JPMC, no travel and expense costs will be reimbursed by JPMC.

b) JPMC will only reimburse Supplier for actual, ordinary, necessary and reasonable travel and expense costs. The reasonableness of any expense shall be determined by JPMC in its sole and complete discretion. JPMC and Supplier must specify in the applicable Schedule or Task Order the maximum amount that JPMC will reimburse.

c) Unless otherwise authorized by the JPMC Relationship Manager or JPMC Project Manager with appropriate authority, a Supplier shall not submit for reimbursement any amount which exceeds the limits previously authorized by JPMC. For purposes of this Policy, the terms JPMC Relationship Manager and JPMC Project Manager will jointly and severally be referred to as the "JPMC Manager".

1) TRAVEL EXPENSES

No "per diems" or other daily allowances are allowed in the U.S. Per diems and/or other daily allowances in non-U.S. locations will be evaluated on a case-by-case basis and must be pre-approved by the JPMC Manager in writing. Evidence of expenditure (e.g., original receipt) is required to be retained by Supplier for any individual expenditure over U.S. $25 and shall be provided to JPMC upon request.

2) AIR TRAVEL

Supplier Personnel must fly in economy or coach class and select the Lowest Logical Airfare ("LLA") which allows the Supplier Personnel to meet JPMC business objectives. LLA is the lowest priced, non-stop flight on any major carrier within a two-hour window of the requested departure or arrival time. If there is no non-stop available flight, the LLA is the lowest priced connecting flight that does not increase the total travel time by more than one-hour over the requested connecting flight.

Supplier must provide an explanation to the JPMC Manager upon submission of reimbursement if the actual fare used exceeds the LLA. If the fare difference is $250 or more, Supplier must get an additional written approval from the JPMC Manager prior to ticketing, or the difference in price will not be reimbursed.

JPMC will not reimburse Supplier for first or business class travel expenses, except as follows:

- **Domestic** (within U.S. or Canada): One class upgrade on overnight flights with work the next day
- **International** (travel within Latin America, Asia Pacific, Middle East and Africa): Business class
- **International – Intercontinental** (e.g. Singapore – U.K.): Business class

Air travel is prohibited between New York and the following: Trenton, NJ; Wilmington, DE; and Philadelphia, PA.

JPMC will not reimburse any additional costs related to the accrual or administration of frequent flyer or other benefits.

If Supplier Personnel receive a full or partial refund from an airline for a business trip paid by JPMC, the refund must be paid to JPMC. This refund policy pertains to cash refunds, corporate credit card refunds and airline vouchers, where applicable.

Reservations should be made as far in advance as possible (i.e., at least two weeks prior to travel). Non-refundable tickets should be utilized whenever possible. Non-refundable tickets or applicable change fees will not be reimbursed if a trip is changed or canceled and the ticket cannot be re-used for JPMC-related business. Lost ticket application fees, extra leg room fees and charges for travel and luggage insurance are not reimbursable expenses. JPMC will reimburse reasonable baggage fees for one bag only.

If Supplier Personnel are assigned a JPMC Standard ID, such personnel must call Carlson Wagonlit Travel ("CWT")

directly at 800.294.4625 (U.S.) in order to utilize JPMC travel discounts for JPMC business-related travel. Supplier Personnel outside the U.S. should engage the JPMC Manager to obtain an appropriate CWT phone number.

3) GROUND TRANSPORTATION

Supplier Personnel should utilize the most cost-effective mode of transportation for their destination, keeping in mind safety for the particular location. Ground transportation will be reimbursed for shuttle, bus, and taxi or car rental subject to this Policy. If a rental car is necessary and approved by the JPMC Manager, an intermediate/mid-size car is the standard. It is Supplier and Supplier Personnel's responsibility to obtain and maintain appropriate levels of auto isurance. JPMC will not reimburse for any auto insurance costs.

Parking, taxi, gas and toll expenses will be reimbursed to the extent that they are necessary and reasonable. Rental cars should be re-fueled prior to return. Fines for parking, traffic violations or towing charges will not be reimbursed. If JPMC reimburses for a rental car and fuel costs, JPMC will not reimburse for driven mileage. Car service is prohibited (except in the UK after 10pm, New York after 9pm and Brooklyn after 8pm with JPMC Manager approval).

4) MEALS & LODGING

Reimbursement for overnight lodging will be provided only if the overnight lodging is a JPMC business-related requirement and specifically pre-approved by the JPMC Manager. Supplier Personnel are to use standard single hotel accommodations at the prevailing commercial rates within a reasonable distance from the destination location. The use of high-priced rooms, suites, executive floors or concierge levels is not reimbursable. Hotels over $300/night require the pre-approval by the JPMC Manager. Non-refundable lodging commitments or applicable change fees will not be reimbursed if a trip is changed or canceled. No-show charges incurred by failing to cancel unused hotel reservations will not be reimbursed.

JPMC will reimburse up to $65 per day for meals, including tax and tip (Breakfast - $10, Lunch - $15 and Dinner - $40). JPMC does not reimburse for lunch unless you typically bring your lunch each day to work or there is no JPMC cafeteria available. In the U.S., tipping up to 15% is warranted for good service and only exceptional service warrants a 20% tip. For non-U.S. locations, tipping should be calculated in accordance with reasonable and customary practices in the applicable location. If a hotel is utilized that offers free breakfast, additional breakfast expenses will not be reimbursed.

5) RAIL TRAVEL:

Class of Service, Domestic or International is as follows:

- Economy/coach: trip that is 3 hours or less
- Business class: trip that is more than 3 hours

Exception: Business First when traveling on Eurostar between London/Paris and London/Brussels

Where customary, tickets for domestic rail travel should be purchased at the point of departure. When traveling on Amtrak in the U.S. and Canada, Supplier Personnel must book reservations at least three days in advance (when possible) directly with Amtrak via the Amtrak web site and obtain tickets at a train station kiosk. For non-Amtrak rail travel, Supplier Personnel should take reasonable steps to book reservations in advance via the lowest cost method (e.g., online).

6) PARKING EXPENSES

Parking expenses incurred during business travel are reimbursable.

7) PHONE EXPENSES

Phone expenses are not reimbursable by JPMC and should be at Supplier's or Supplier's Personnel's cost. If JPMC requires Supplier Personnel to travel internationally, JPMC will reimburse reasonable phone expenses (i.e. JPMC business-related and daily check-in with family) with prior written approval from the JPMC Manager. The lowest cost options should be utilized.

8) OTHER EXPENSES

All other expenses should be authorized by the JPMC Manager prior to incurring such expenses. Otherwise such expenses will not be reimbursed. Non-reimbursable items include but are not limited to the following:

- Barber/hairstyle fees
- Car washes, repairs, towing, and other types of maintenance
- Clothing, toiletries or medications
- Finance charges
- Fuel charges for personal vehicles
- Health clubs & beauty spas
- Personal housekeeping expenses while traveling for JPMC business
- Late fees of any kind
- Laundry and dry cleaning services if traveling less than 6 consecutive nights
- Medicine of any type (expect for required international travel)
- Alcohol or other expenses of a personal nature
- Mini-bar/refreshment center charges
- Personal entertainment (newspapers, magazines, movies, etc.)
- Shoe repair
- Traffic violations, parking tickets, and related court costs
- Unexplained, excessive unreasonable or lavish expenses
- Uniforms

9) LOCAL TRAVEL

In order to provide cost-effective services to JPMC, Supplier shall use best efforts to supply qualified local personnel for performance of services for JPMC to the extent reasonably possible. JPMC shall have no responsibility to reimburse any travel expenses performed by local personnel supplied by Supplier. For the purposes of this Policy, the term "local" shall mean residence or Supplier designated office of the applicable personnel within a fifty (50) mile radius of the location where the applicable services are performed.

10) INTERNATIONAL TRAVEL

For international travel, currency exchange rates shall be indicated in all invoices or statements. Fees for currency conversion shall not be reimbursed. All expense limits in this Policy are in U.S. dollars. For international travel, the expense limit should be adjusted by the applicable exchange rate. Where appropriate, such as lower cost countries, any expenses submitted to JPMC for reimbursement should not exceed commercially reasonable rates for the international location.

11) REIMBURSEMENT

Supplier Personnel are to use their own personal or company credit card for travel expenses, and Supplier must submit an invoice to the JPMC Manager for reimbursement in accordance with the applicable Supplier agreement or purchase order terms and conditions. Submissions to the JPMC Manager for reimbursement must **reference a valid purchase order** or **valid Schedule referencing a valid Master Agreement**. Reimbursement requests and invoices which do not reference a purchase order or a Schedule (include CW#_____) will be rejected or returned to the Supplier. All expense claims shall be submitted within 10 days after the beginning of each month and no later than one (1) month after the date the actual expense was incurred. Spousal travel costs will not be reimbursed.

12) TRAVEL TIME

Travel time is not a reimbursable expense and will not be paid by JPMC.

13) GENERAL MINIMIZATION OF COSTS

JPMC would like to have very communicative relationships with its Suppliers and is always open to discussing lower cost options. If certain travel circumstances may be more beneficial to Supplier and JPMC yet would be exceptions to the Policy, JPMC may but is not obligated to consider such exceptions.

February 2015

USA Vendor Pre-Engagement Screening (PES) Initiation Guide

Category 2 Supplier Personnel

(Exception Basis)

Last Update: July 23, 2021

Copyright ©2021. All Rights Reserved. JPMorgan Chase Bank, N.A. Proprietary Information

Overview

Pre-Engagement Screening (PES) is conducted on an exception basis for select suppliers as approved at JPMC's sole discretion.

These instructions are to be followed for select Contingent Workers (i.e., Category 2 Supplier Personnel) who do not require an ID Badge but provide a service to JPMC that may require them to have access to JPMC data or property or its customers (tangible or intangible) and who are not considered Category 1 Supplier Personnel.

Screening requires workers to get fingerprinted for a criminal background check.

For Technical Issues regarding your FBI Consent application, please contact:

- Application Station Help: 1 (888)-291-1369 ext. 2006

For Technical Issues regarding your fingerprint appointment, please contact:

- Fieldprint Help: +1 (877)-614-4362

For General Questions, please contact JPMC Global Workforce Screening team:

- Telephone: 1 (201)-595-5200
- Email: GWS.Contingent.Workers@chase.com

NOTE: Additional screening will be required if access to JPMC systems and/or ID Badge is needed.

All Personnel must be fingerprinted and cleared by Global Workforce Screening prior to their assignment with JPMorgan Chase.

JPMC will only disclose eligibility for assignment at JPMorgan Chase – no details of the screening results will be provided to the Supplier.

Copyright ©2021. All Rights Reserved. JPMorgan Chase Bank, N.A. Proprietary Information

United States Pre-Engagement Screening Instructions

Pre-Requisites:

When filling out the application, follow these important instructions:

- Use full Legal name on application
- Confirm you enter the correct Social Security Number
- You MUST include an applicable JPMC Cost Center
- Provide Agency name; the company you are directly employed by

Step 1: Capture FBI Consent:

1. Supplier instructs candidate to visit Application Station 2.0 site.
2. Enter code "**FPCVENDOR**" in the Application Station Code section
3. Complete all required fields and sign Consent
4. Submit Application

Note: it is an FBI requirement to capture this consent form specifying the purpose of why JPMC is collecting fingerprints. This step must always be performed BEFORE scheduling an appointment in step 2.

Step 2: Schedule Fingerprint Appointment:

1. Supplier instructs candidate to visit Fieldprint site.
2. Worker creates an account by clicking "Schedule an Appointment"
3. Once signed in, use the Fieldprint code **FPCVENDOR**
4. Complete personal and demographic information (must use legal name)
5. The following fields are required:
    - Agency Name
    - Billing Code/Cost Center
6. Candidate can now schedule his or her appointment

See next section for detailed step-by-step guidance on completing this application.

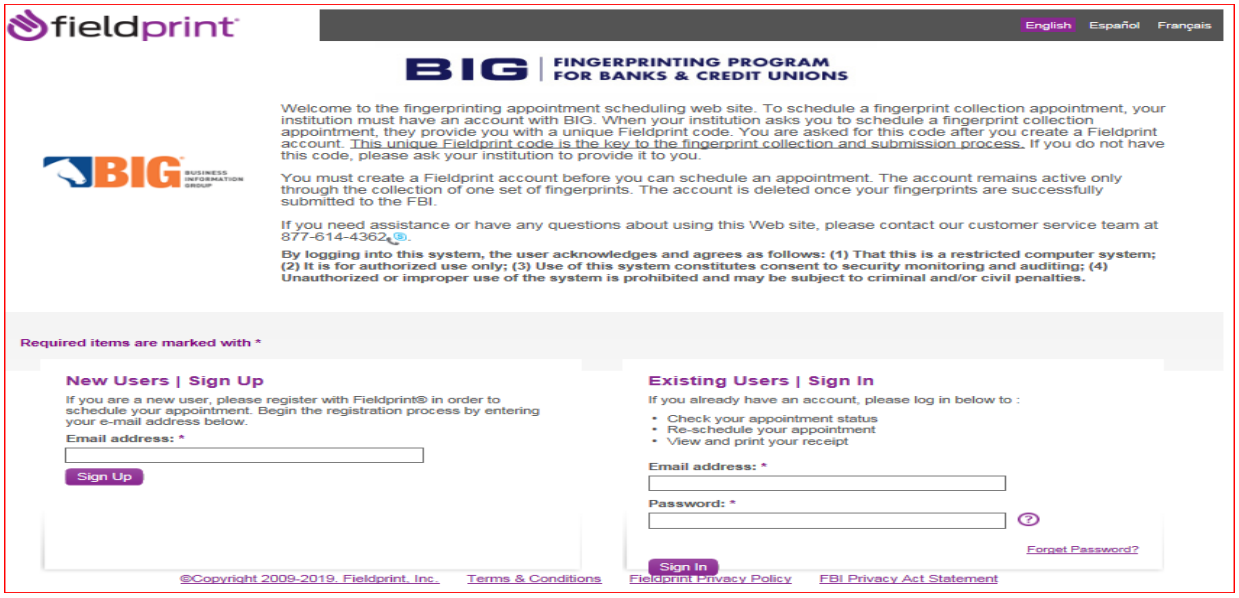
Note: The screening turn-around-time varies from 2 to 10 business days or more, depending upon a worker's responsiveness to any requests for additional information.

Copyright ©2021. All Rights Reserved. JPMorgan Chase Bank, N.A. Proprietary Information

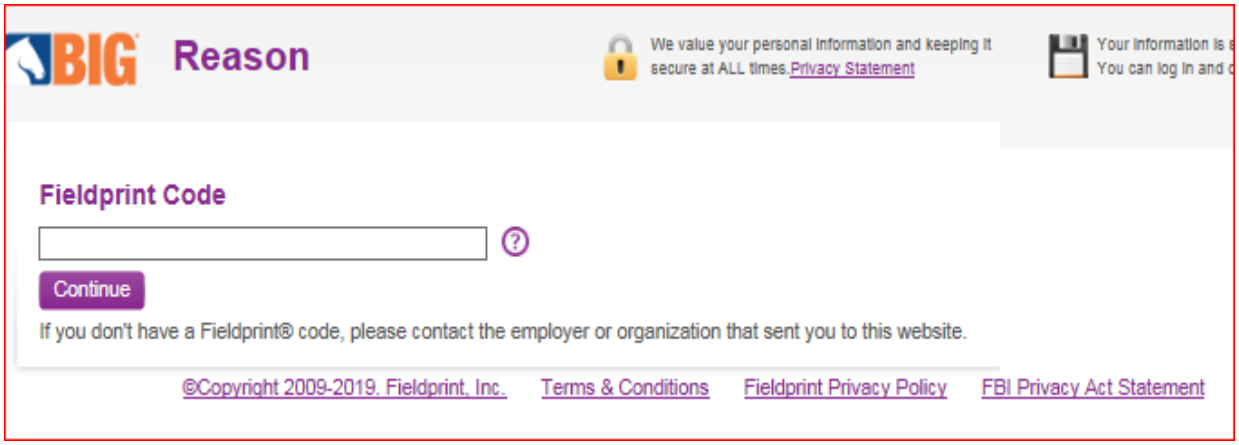
Step-by-Step Instructions

Account Creation:

1. Click the Fieldprint link to access the online appointment scheduler
2. Once on the application page, you will be required to make an account by filling out all necessary fields



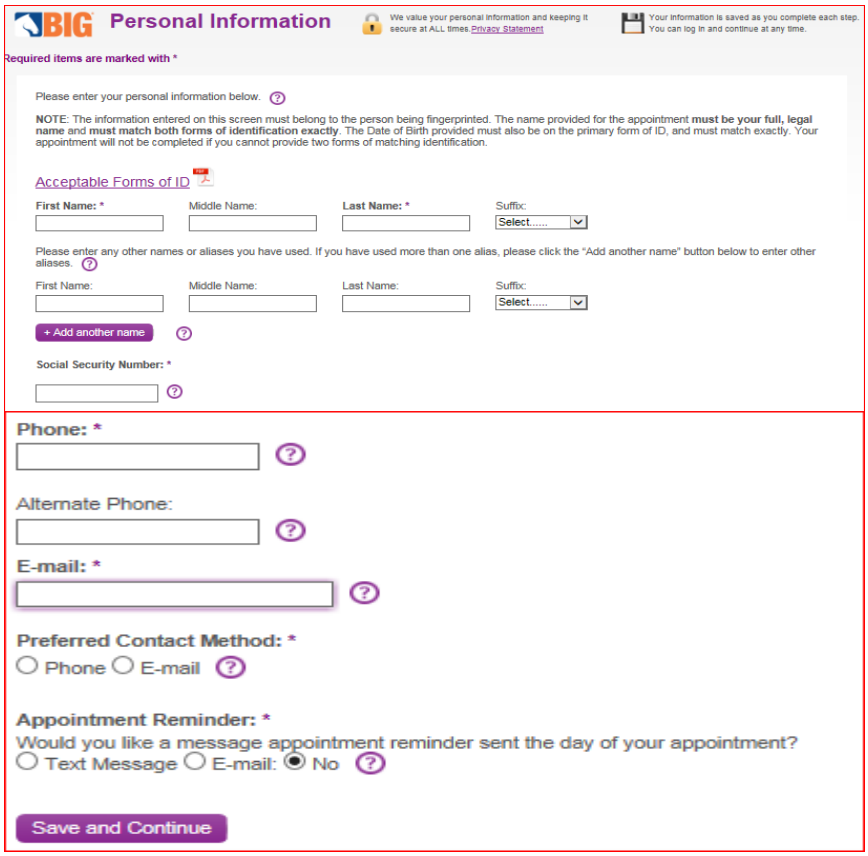
3. After account creation, you will be prompted to enter a Fieldprint Code. Use **FPCVENDOR**



Copyright ©2021. All Rights Reserved. JPMorgan Chase Bank, N.A. Proprietary Information

Application Section 1: Personal Information

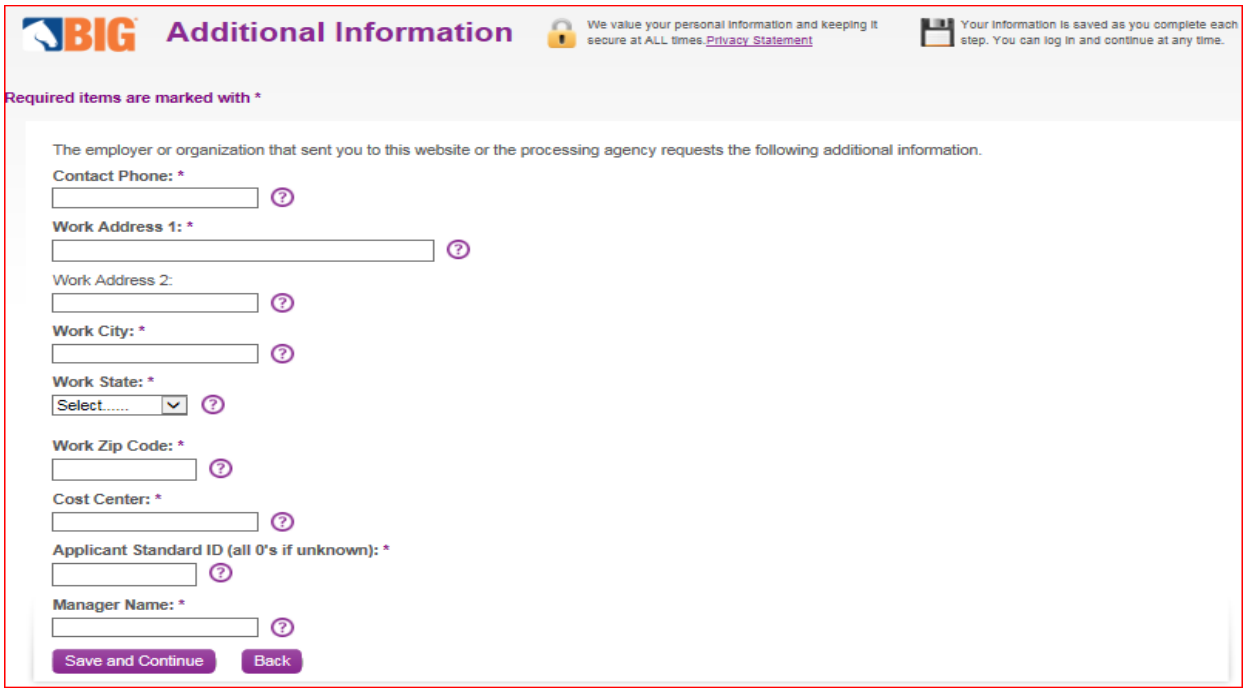
1. Fill out the entire Personal Information section of the application



Copyright ©2021. All Rights Reserved. JPMorgan Chase Bank, N.A. Proprietary Information

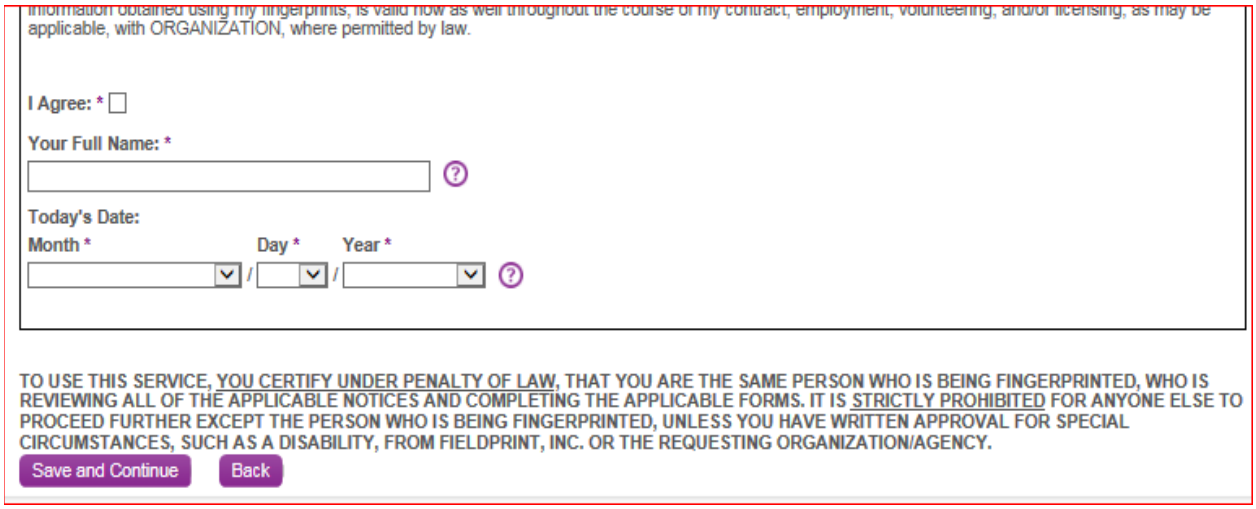
Application Section 2: Additional Information

1. Fill out all required fields marked with *



Application Section 3: E-consent Waiver

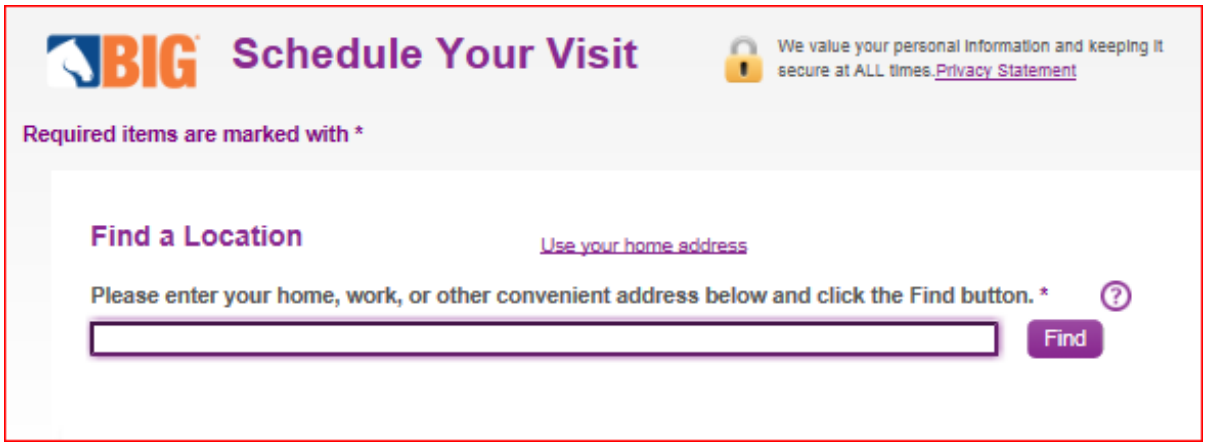
1. Click Agree and complete information. You can click "Save and Continue"



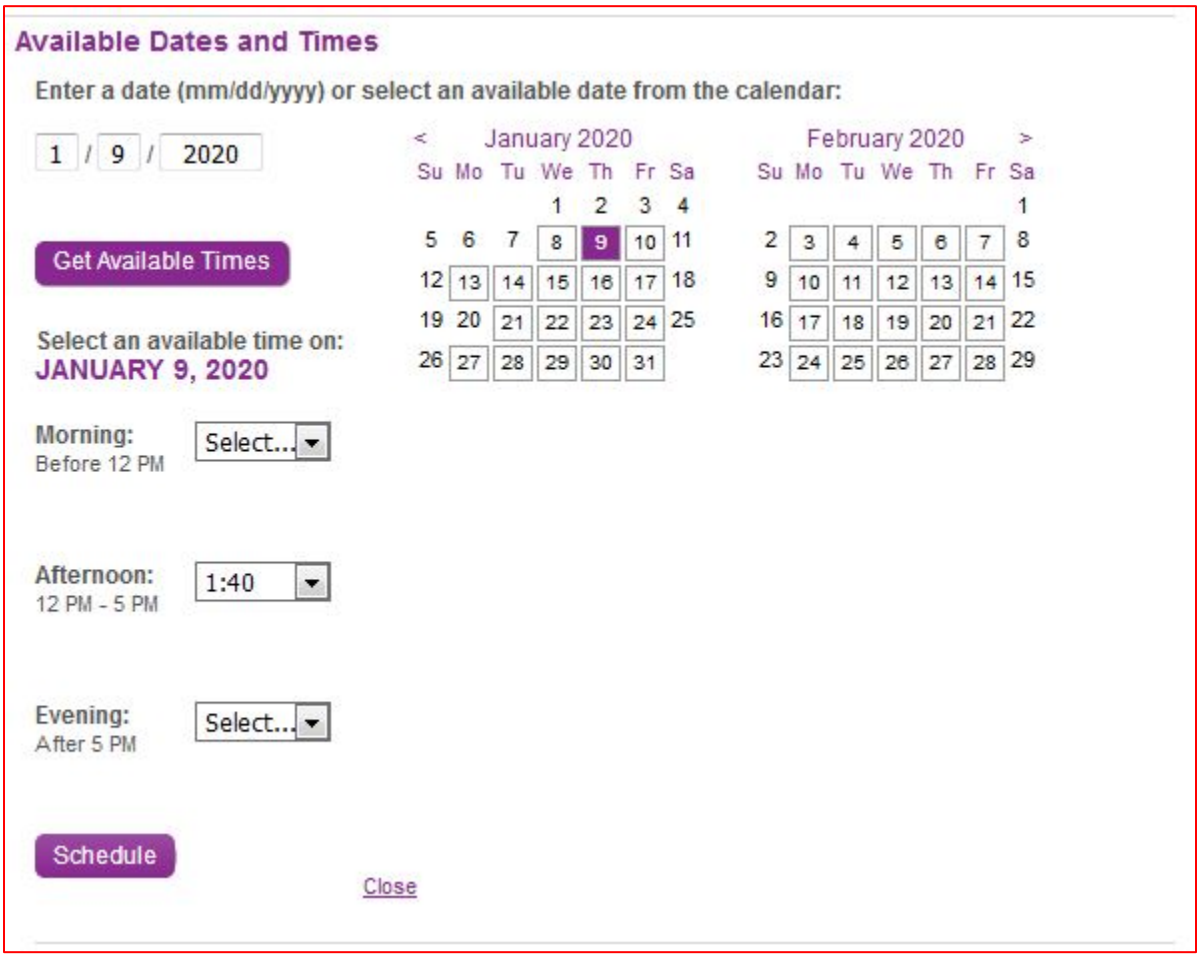
Copyright ©2021. All Rights Reserved. JPMorgan Chase Bank, N.A. Proprietary Information

Application Section 4: Schedule Your Visit

1. Enter an address or zip code to find nearby locations and select a desired fingerprint location

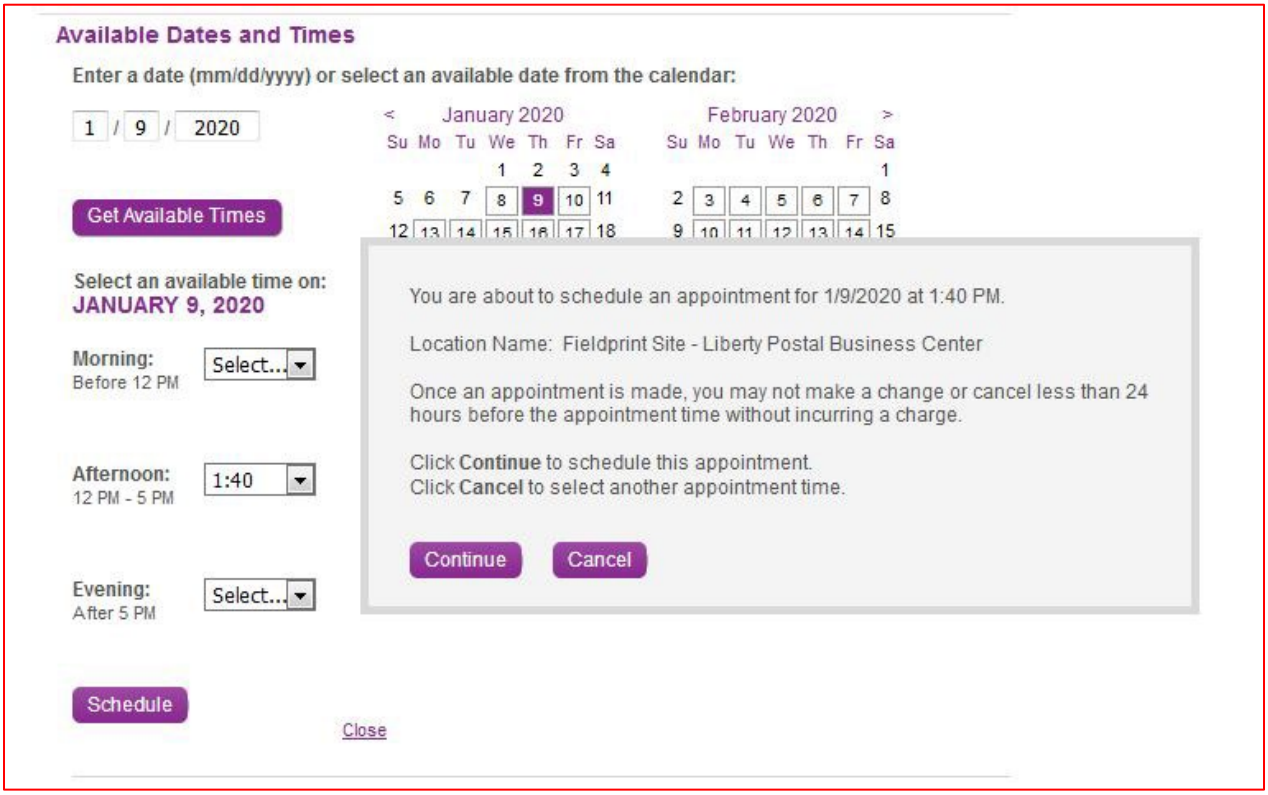


2. Select your fingerprinting appointment date and time and click the "**Schedule**" button



Copyright ©2021. All Rights Reserved. JPMorgan Chase Bank, N.A. Proprietary Information

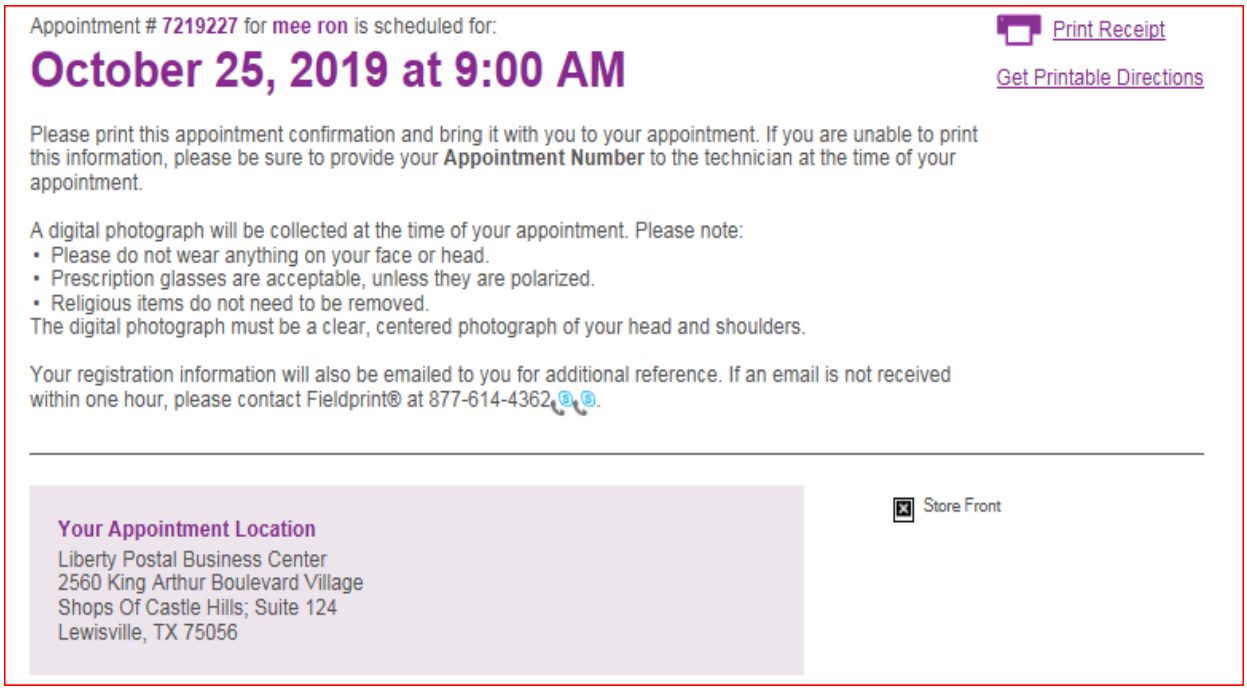
3. After clicking “Schedule”, you will be prompted to verify the appointment details are correct. The appointment will ONLY be scheduled once you click “Continue” on this prompt



Copyright ©2021. All Rights Reserved. JPMorgan Chase Bank, N.A. Proprietary Information

Application Confirmation

1. Save your confirmation details after booking your appointment. You will also receive an e-mail confirmation



Copyright ©2021. All Rights Reserved. JPMorgan Chase Bank, N.A. Proprietary Information

CONTROLLER - TO - CONTROLLER SCCs

PART 1

STANDARD CONTRACTUAL CLAUSES

SECTION I - INITIAL PROVISIONS

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'); and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: "**Clauses**").

(c) these Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) the Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.5 (e) and Clause 8.9(b);

(iii) Reserved

(iv) Clause 12(a) and (d);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause – deleted.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain: (i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned); (ii) its likely consequences; (iii) the measures taken or proposed to address the breach; and (iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points (ii) to (iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter "**sensitive data**"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "**onward transfer**") unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9

Reserved

Clause 10

Data subject rights

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request (FN10: That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests). The data

importer shall duly and promptly inform the data subject of any such extension.. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter "**automated decision**"), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination – including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights (or where exporter does not have an establishment in an EU Member State), they shall be governed by the law of Germany.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the EU Member State in which the data exporter is established, or if exporter does not have an establishment in an EU Member State, Germany.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

The following Annexes form part of the Clauses.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Name: JPMorgan Chase Bank, N.A.

Address: 383 Madison Avenue, New York, New York 10179, United States

Contact person's name, position and contact details: As specified in the Agreement.

Activities relevant to the data transferred under these Clauses: As specified in the Agreement.

Signature and date: The parties agree that execution of the Agreement by the data importer and the data exporter shall constitute execution of these Clauses by both parties as follows: (a) on 27 October 2021, where the effective date of the Agreement is on or before 27 September 2021, or (b) otherwise, on the effective date of the Agreement.

Role: Controller

2. **Data importer(s)**:

Name: As specified in the Agreement.

Address: As specified in the Agreement.

Contact person's name, position and contact details: As specified in the Agreement.

Activities relevant to the data transferred under these Clauses: In accordance with the Deliverables provided under the Agreement.

Signature and date: The parties agree that execution of the Agreement by the data importer and the data exporter shall constitute execution of these Clauses by both parties as follows: (a) on 27 October 2021, where the effective date of the Agreement is on or before 27 September 2021, or (b) otherwise, on the effective date of the Agreement.

Role: Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Concern current / former/ prospective employees; current / former / prospective wholesale clients; current / former / prospective retail clients; visitors to websites / online services, or as otherwise described in the Agreement.

Categories of personal data transferred

Personal Data including data relating to data subjects provided to the Supplier in connection with the Deliverables by or at the direction of JPMC or as otherwise described in the Agreement.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The frequency of the transfer shall be as described in the Agreement.

The nature of the processing shall be as described in the Agreement.

The purpose(s) of the data transfer and further processing shall be as described in the Agreement.

The period for which the personal data will be retained, or the criteria used to determine that period shall be as described in the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

The Supervisory Authority of Hesse, Germany

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Importer shall comply with the measures set out in JPMC's security policies in force from time to time, including JPMC's Minimum Control Requirements, a current copy of which is located at:

https://www.jpmorganchase.com/about/suppliers/guidelines-documents

or as otherwise specified in the Agreement.

ANNEX III

List of Subprocessors

N/A

Covered Jurisdiction ex-UK – ADDENDUM

Where:

A. the entity exporting data is an entity not established in any Member State of the European Union (excluding the UK);

B. the entity exporting data is subject to the law of the country in which it is established ("**Applicable Law**"); and

C. JPMorgan Chase Bank, N.A. and data importer have entered into the Standard Contractual Clauses in respect of the transfer of personal data from the entity exporting data to the data importer as more particularly described in Annex I to the Standard Contractual Clauses, the parties hereby agree as follows:

1.1 the terms of the Standard Contractual Clauses are amended as follows:

(a) the terms "personal data", "special categories of data", "process/processing", "controller", "processor", "data subject", "supervisory authority", "Data Protection Authority", "automated decision", "personal data breach" and "third country" shall be interpreted in accordance with their equivalent terms in Applicable Law;

(b) all references to the term "**Member State**" shall be deleted and replaced with "**country**";

(c) all references to "**Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)**", including references to "**Regulation (EU) 2016/679**", "**GDPR**" and/or any references to the articles of Regulation (EU) 2016/679 shall be deleted and replaced with "**Applicable Law**" or the "relevant principles consistent with Applicable Law" where Applicable Law does not expressly provide for the indicated ; and

1.2 the parties shall comply with the provisions of Applicable Law at all times in relation to the transfers contemplated under the Standard Contractual Clauses as more particularly described in Annex I; and

1.3 in the event that there is any conflict between Applicable Law and the Standard Contractual Clauses, Applicable Law shall govern;

1.4 rights and obligations provided in the Standard Contractual Clauses shall apply only to the extent provided for under Applicable Law; and

1.5 Clause 17 shall read "These Clauses shall be governed by the law of the country in which the data exporter is established.". The remainder of Clause 17 shall be deleted; and

1.6 for purposes of Annex IC, the competent supervisory authority shall be the supervisory authority of the country in which the data exporter is established.

Covered Jurisdiction - UK ADDENDUM

UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers of data from the UK subject to the UK GDPR. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract. The following Addendum forms part of the Addendum EU SCCs.

Part 1: Tables

Table 1: Parties

Start date	Data importer and data exporter shall be deemed to have executed these Clauses effective of the following date: (a) on 27 October 2021, where the effective date of the Agreement is on or before 27 September 2021, or (b) otherwise, on the effective date of the Agreement.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	As indicated in Annex I.A	As inidcated in Annex I.A
Key Contact	As indicated in Annex I.A	As indicated in Annex I.A
Signature (if required for the purposes of Section 2)	Not required.	Not required.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: As above. Reference (if any): N/A Other identifier (if any): N/A

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: As above.
Annex 1B: Description of Transfer: As above.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As above.
Annex III: List of Sub processors (Modules 2 and 3 only): N/A

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☒ Exporter ☐ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.

Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

> "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

c. Clause 6 (Description of the transfer(s)) is replaced with:

> "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

> "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

> "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

> "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

> "These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

> "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a its direct costs of performing its obligations under the Addendum; and/or

    b its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

JPMC'S MINIMUM CONTROL REQUIREMENTS FOR CONTINGENT LABOR SUPPLIERS

These Minimum Control Requirements ("**Minimum Control Requirements**") are stated at a relatively high level, and JPMC recognizes that there may be multiple approaches to accomplish a particular Minimum Control Requirement. Supplier must document in reasonable detail how a particular control, including those pertaining to dependent third party providers (subcontractors) who collect, transmit, share, store, control, process, manage or access JPMC Data, meets the stated Minimum Control Requirement. The term "**should**" in these Minimum Control Requirements means that Supplier will use commercially reasonable efforts to accomplish the stated Minimum Control Requirement, and will document those efforts in reasonable detail, including the rationale, if any, for deviation. This documentation may be reviewed by Auditors to assess the control and the merit of the rationale for deviation. Not all of the stated Minimum Control Requirements will apply to all Services or other Deliverables, but Supplier must be able to reasonably show how the Minimum Control Requirement does not apply. These Minimum Control Requirements do not limit Supplier's obligations under the Agreement or applicable Law, and do not limit the scope of an audit by JPMC.

In addition to these Minimum Control Requirements and provisions stated in the Master Services Agreement, some Suppliers have agreed to and signed "Rules of Engagement" regarding interactions between Supplier Personnel and JPMC in the provision of staffing services. These "Rules of Engagement" continue to be in force and are not replaced by, but are requirements in addition to, these Minimum Control Requirements.

As used in these Minimum Control Requirements, (i) "**including**" and its derivatives mean "including but not limited to", and; (ii) any capitalized terms not defined herein shall have the same meaning as set forth in the applicable Master Services Agreement.

CANDIDATE SOURCING

High-level control objective:

Supplier's compensation of recruiters is appropriate and does not incent the placement of unqualified or otherwise inappropriate candidates. Supplier has a robust program to monitor and assess performance of any Supplier Personnel and/or subcontractors used for candidate sourcing or for verification services (background, education and employment) and skill assessments.

Recruiting:

Supplier's recruiting process must be documented and must demonstrate that compensation practices are based on successful placement of candidates. Process must include actions taken and subsequent performance monitoring of recruiters when those recruiters demonstrate a pattern of placing candidates with early terminations including issues of unacceptable performance, job abandonment, early resignations or negligible or fraudulent conduct.

Supplier must maintain data on candidate placement, early terminations and early and on-time releases and extensions for a period of three years following assignment completion or termination and that provide that data upon request.

Recruiters should be subject matter experts in their areas of concentration and/or highly experienced in recruiting. If requested, recruiters' experience and resumes should be made available to JPMC assignment sponsors.

Referrals:

The Supplier's referral program, and any corresponding incentives, must be documented and available for review.

Supplier referral process must ensure that referred candidates are appropriately experienced and skilled before they are put forth for any role. Referrals include candidates referred by Supplier Personnel and candidates referred by external sources. The referral process should be designed so that referrals are accepted only from Supplier Personnel with a successful tenure of six months or more and that referral incentives are not a substitute for active and diligent recruiting efforts. Referral incentives, if any, should be paid out only after a defined waiting period to ensure the referred candidate's success in the role.

Supplier must track referrals be able to provide information on the frequency of referrals in general, and on the source of the referral, on any referred candidates. All referrals must be categorized as either (i) referred by JPMC employee or client, (ii) referred by Supplier Personnel, (iii) referred by External Party – Government Official or (iv) referred by External Party – Other. Additionally, JPMC must be informed at the time of resume provision, which candidates have been referred and which have been obtained through the standard candidate sourcing process.

Subcontractors:

Supplier must not use subcontracted recruiters or staffing firms in sourcing candidates for JPMC without prior written approval, which JPMC may withhold in its sole discretion.

Subcontractors may be used to verify background, education and/or references and to administer capability assessments. The Supplier must review documentation related to any candidate verification and must

maintain copies of all documents for a period of seven years following the completion or termination of the assignment. Suppliers must be able to evidence their review of candidate verification, inclusive of document copies, before any candidate is put forth to JPMC.

CANDIDATE SKILLS ASSESSMENT

High-level control objective:

Supplier's end to end process ensures that identified candidates have the skills, experience, training and qualifications to perform the requested functions. Following the initial phone screening, all candidate interviews should be conducted either in person or via video.

Supplier must have a process to identify and assess skills and competencies of candidate(s) that are relevant for the role, including situational questions and technical tests as appropriate. The process must include dispositioning of failing test results. Assessment results must match the skills and capabilities described on the candidate's resume. Supplier should develop a testing curriculum for key skills designed to be comprehensive with a passing result providing assurance to JPMC that the candidate is qualified. No unqualified candidates are to be presented to JPMC. Testing results must be made available to JPMC upon request and assessments for required role skills should be assessed within 12 months prior to placement at JPMC, except if a candidate was formerly at JPMC within the past 12 months and will be placed in a role requiring the same skills as the prior role. Any other requested exceptions to testing requirements must be approved in writing by JPMC.

The Supplier process must also include a method to verify at the time of testing that the candidate taking the test is the candidate. Testing results (including dates and scores) and identity verification data must be made available upon request and retained for a period of three years following the completion or termination of the assignment.

CANDIDATE BACKGROUND SCREENING

High-level control objective:

The Supplier hiring process must include a documented process for the performance of any and all checks necessary to ensure that placement of a candidate at JPMC will not expose JPMC to fraud, theft, negligence or violence.

In addition to employment and education verification as described below, background screenings must be completed within 90 days before placement at JPMC and must include the following, where allowed by law:

Criminal check
I-9 Verification/ or equivalent eligibility documentation if outside of the US.
Social Security/Identity Check
Drug Screening

Results of all background screening must be maintained for as long as the candidate assignment is ongoing and for an additional three years following the completion or termination of the assignment. If the candidate is placed at JPMC for a second or subsequent time and 90 days or more has elapsed since the completion or termination of the last assignment, the entire background screening process must be performed again before placement.

CANDIDATE EDUCATION AND REFERENCE VERIFICATION

High-level control objective:

Supplier's end to end process ensures that identified candidates have accurately and completely described prior job experience and attained education.

Supplier must have a robust process to verify the highest level of education listed on the application and/or resume of candidate. Additionally, Supplier must verify all relevant work experience for the past 10 years.

Verification should include the following components:

Education:

Candidate attended and graduated from all schools indicated as highest level of education
Candidate earned the degree/certification indicated
Candidate has completed all certification continuing education requirements indicated (if applicable)

Work Experience:

Candidate held the role/title indicated
Candidate worked at the stated company for the time indicated

CANDIDATE IDENTITY VERIFICATION

High-level control objective:

Assurance that throughout the Supplier screening process, the identity of the candidate is verified and recorded at multiple checkpoints, particularly at interview, during any capabilities assessment and at the start of each work assignment.

Suppliers must have a documented process to verify candidate's identity by examining and recording multiple sources of identification. Suppliers must maintain all onboarding and identity verification paperwork, including copies of documents examined to confirm candidate identity for a period of 3 years following the completion or termination of the assignment.

SUPPLIER PERSONNEL PERFORMANCE MONITORING

High-level control objective:

The Supplier must have a process to collect feedback periodically from JPMC to ensure that the performance of Supplier Personnel is meeting expectations.

SUPPLIER PERSONNEL CONDUCT TRAINING AND ATTESTATIONS

High-level control objective:

The Supplier Personnel hiring program must include Code of Conduct and Anti-Corruption training to ensure resources are fully aware of conduct requirements at JPMC.

Suppliers must provide adequate training on the JPMorgan Chase & Co. Supplier Code of Conduct, along with supplier developed training on Cyber Security and Phishing, compliance with applicable laws, and the proper provision of Services and privacy training prior to commencing work at JPMC.

Candidates must attest to the completion of required training on an annual basis. Supplier is responsible for maintaining current candidate attestation records.

REGULATORY AND LEGAL COMPLIANCE

High-level control objective:

Supplier must have a structure and processes in place for researching, evaluating, and complying with all National and other Laws and regulations that are relevant to Recruitment, Hiring Practices, and Employment Law in addition to all other legal and regulatory requirements impacting the services provided.

Supplier must be compliant with any applicable laws and regulations for JPMC Data to include candidate information that is stored, managed, shared, or accessed by the Supplier and its subcontractors.

Supplier must have reporting requirements for supplier personnel if they are arrested. All arrests must be reported, with the exception of minor traffic violations/citations. All supplier personnel must notify their employer regarding any current arrest/pending charges and provide supporting documentation related to the matter. Supplier must promptly notify JPMC if any current resources report an arrest or pending charges.

EUROPEAN PRIVACY ADDENDUM

1. In respect of personal data relating to individuals located within EMEA that is included in the Customer Data and processed by Supplier pursuant to the Agreement, Supplier shall at all times act as a data processor in respect of such personal data. For the avoidance of doubt this Privacy Addendum shall be applicable to all countries in the EMEA region which includes but is not limited to all countries in the European Ecomonic Area, Switzerland, South Africa, Israel, Turkey, Nigeria and Kenya.

2. The provisions of this Addendum and the EU Model Clauses executed by Supplier and JPMorgan Chase Bank, N.A on behalf of its affiliates pursuant to this Addendum and attached hereto shall override and have precedence over any contrary provisions in the any Agreement.

3. For the purposes of this Addendum, the terms "personal data", "data processor", "special categories of data" and "processing" shall have the same meanings as are given to those terms in European Directive 95/46/EC (as it may be amended from time to time) and the definitions in Applicable Law in the relevant countries to protect all information within scope of such laws and shall be interpreted accordingly.

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: JPMorgan Chase Bank, N.A

Address: 270 Park Avenue, New York, New York 10017, United States

Tel.: ……..……..; fax: ……..……..;

e-mail: ……..……..……..…..……..

Other information needed to identify the organisation

……

(the **data exporter**)

And

Name of the data importing organisation: ……..……..……..……..……..……

Address:

……..……..……..……..……..……..……..

……

Tel.: ……..……..; fax: ……..……..;

e-mail: ……..……..……..…..……..

Other information needed to identify the organisation

……

(the **data importer**)

each a "party" and together "the parties"

HAVE AGREED on the following Contractual Clauses (the **Clauses**) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

1. Definitions

For the purposes of the Clauses:

"**personal data**", "**special categories of data**", "**process/processing**", "**controller**", "**processor**", "**data subject**" and "**Supervisory authority**" shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

the "**data exporter**" means the controller who transfers the personal data;

the "**data importer**" means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of

Article 25(1) of Directive 95/46/EC;

the "**subprocessor**" means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

the "**applicable data protection law**" means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member Jurisdiction in which the data exporter is established;

"**technical and organisational security measures**" means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2. Details of Transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

3. Third-party Beneficiary Clause

The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (b), Clause 7, Clause 8(2) and Clauses 9 to 12, as third-party beneficiary.

The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4. Obligations of the Data Exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions

of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member Jurisdiction where the data exporter is established) and does not violate the relevant provisions of that Jurisdiction;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or a soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 83 to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subject upon request a copy of the Clauses , with the exception of Appendix 2 and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

5. Obligations of the Data Importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled

to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy of the data exporter:

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

6. Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any

party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph (a) against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has became insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity..

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issues a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operation under the Clauses.

7. Mediation and jurisdiction

1 The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member Jurisdiction in which the data exporter is established.

(c) The parties agree that the choice made by the data subject will not prejudice his substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

8. Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of

an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

9. Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, United Kingdom, Estonia, Finland, France, Germany, Greece, Guernsey, Hungary, Ireland, Italy, Jersey, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovak Republic, Slovenia Spain, Sweden, Switzerland as applicable.

10. Variation of the Contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business-related issues where required as long as they do not contradict the Clause.

11. Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written consent between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph (a) shall be governed by the law of the Member State in which the data exporter is established, namely Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, United Kingdom, Estonia, Finland, France, Germany, Greece, Guernsey, Hungary, Ireland, Italy, Jersey, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovak Republic, Slovenia Spain, Sweden, Switzerland as applicable.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

12. Obligation after the Termination of Personal Data Processing Services

1. The parties agree that on the termination of the provision of data processing

services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, he will submit its data processing facilities for an audit of the measures referred to in paragraph (a).

On behalf of the data exporter:

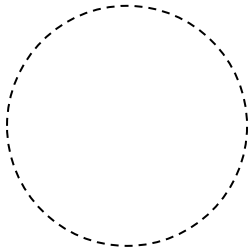
Name (written out in full): .....

Position: .....

Address: .....

Other information necessary in order for the contract to be binding (if any):

.....



(stamp of organisation) Signature .....

On behalf of the data importer:

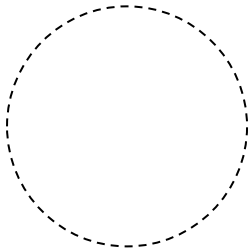
Name (written out in full): .....

Position: .....

Address: .....

Other information necessary in order for the contract to be binding (if any):

.....



(stamp of organisation) Signature .....

APPENDIX 1
to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

A global financial services provider .....

.....

.....

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

A global information technology services provider .....

.....

.....

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

The data transferred may involve all categories of data subjects of the Data Exporter including, without limitation: .....

- Current, past, potential employees, trainees, voluntary workers
- Current, past, potential employees of associated companies, organisations
- Current, past, potential employees of other organisations
- Current, past, potential recipients, customers, counter parties or clients for goods or services (direct or indirect)
- Current, past, potential suppliers of goods or services (direct or indirect)
- Current, past, potential contacts at correspondent banks and other associated financial institutions
- Current, past, potential directors, other senior officers
- Current, past, potential business or other contacts
- Current, past, potential advisors, consultants, professional and other experts
- Current, past, potential correspondents and enquirers
- Current, past, potential elected representatives, other holders of public office
- Current, past, potential survey respondents, other persons assisting research
- Current, past, potential claimants, beneficiaries, payees
- Relatives of all of the above.

.....

.....

Categories of data

The personal data transferred concern the following categories of data (please specify):

Current, past & potential Clients, Counterparties and Suppliers

- Agreements, contracts
- References to manual files and records
- Personal identifiers
- Details of accounts and transactions
- Financial identifiers
- Identifiers issued by public bodies
- Personal details
- Goods, services provided to the Data Subject
- Goods, services obtained from the Data Subject
- Other contracts with Data Subject (not being goods or services)
- Business activities of the Data Subject
- Creditworthiness

Human Resources Information

- Work management details
- Performance assessment and appraisal information
- Court Orders and records regarding wage garnishment, child support agreements and equivalent
- Training record
- Security details
- Pension details
- Compensation, credit history and taxation details
- Recruitment details
- Personal details (including date of birth)
- Career history
- Termination details
- Current marriage or partnership details
- Academic record
- Qualifications and skills
- Membership of professional bodies
- Professional expertise
- Membership of committees
- Current employment status
- Financial transactions
- Insurance details
- Publications
- Internal compliance information
- Career management, budget and compensation planning

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

All categories of sensitive data transferred from the data exporter to the data importer, including without limitation:

- Disabilities, infirmities
- Political affiliations
- Health and sickness
- Health and safety
- Ethnicity
- Dietary requirements
- Criminal convictions and arrests

and such other special categories of data as data subjects may from time to time volunteer to the data exporter.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

- Incidental access during the provision of information technology services by the data importer
- Storage or transport of data on equipment used by the data importer
- Provision of business services of an advisory, consulting or intermediary nature in relation to best practice and benchmarking services

DATA EXPORTER	DATA IMPORTER
Name: …….	Name: .....
Authorised signature: …….....	Authorised signature: .....

APPENDIX 2
to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Those measures set out in JPMC's security policies in force from time to time. JPMC's Minimum Control Requirements a current copy is located at: https://www.jpmorganchase.com/corporate/About-JPMC/document/JPMC_Minimum_Control_Requirements_ada.pdf

Incident Response Procedure – Best Practice Recommendations

Background

This Incident Response Procedure provides a framework for building an incident communication capability within a Supplier organization to communicate the appropriate information and details of a cyber incident in a timely manner to JPMorgan Chase & Co ("JPMC") to meet JPMC's Minimum Control Requirements.

This Incident Response Procedure documents the steps and actions to be taken by the Supplier, and is meant to be used as a general guideline for incidents; however, specific responses and actions must be tailored to the incident, its size, scope and impact. It is not intended to replace or circumvent any of Supplier's existing procedures for the resolution of the actual incident. All of Supplier's other existing policies and procedures must be adhered to for the reporting, communication (regulatory, customer and media) and resolution of the specific incident(s).

Supplier Incident Communication Procedure

A Supplier must establish a formal incident communication procedure ("Response Procedure") to ensure its respective teams are familiar with their responsibilities in the event of an incident. A formal incident communication team made up of subject matter experts ("SMEs") and senior management with the authority & responsibility to communicate with JPMC is essential in timely dissemination of information.

An " incident" that would trigger the Response Procedure is any event which results in (y) unauthorized access to, disclosure or use of, or loss of integrity to (i) JPMC information; (ii) systems that store, process or transmit JPMC information; and/or (iii) systems that are otherwise used to provide JPMC services (including, but not limited to, source code repositories and software delivery systems); or (z) the unavailability of any service provided to JPMC that is a result of malicious activity, as well as any violation or imminent threat of violation of security policies, acceptable use policies, or standard security practices

<u>Response Procedure Testing</u>

1. Have a documented Response Procedure runbook.
2. Test the runbook, through paper based table top exercises and through hands on keyboard simulations.
3. Get pre-approval (or have agreement on a fast approval process) from management and legal to share Indicators of Compromise (IOC) and Tactics, Techniques and Procedures (TTP) with law, government, partners and customers who request it.

Incident Response Procedure – Best Practice Recommendations

Incident Management Actions to be taken by Supplier

The following are the details JPMC will require during the initial communication:

Data Gathering:

1. Document/summarize the incident per table below

JPMC Communications:

1. Based upon immediately available information, Supplier communicates the incident to JPMC within the time frame set forth in the governing agreement with JPMC.
2. How to initially notify JPMC:
    a. Supplier can contact the JPMC Delivery Manager.
    b. Supplier can contact the JPMC Cyber Hotline 24x7 by phone 1877 576 7621; or
    c. Supplier can email Cyber.alert@jpmchase.com or JPMC.Supplier.Notifications@jpmchase.com.
3. Schedule conference call with JPMC Delivery Manager to explain the incident (details per table below) and determine next steps, which will be based on the nature and severity of the incident
    a. Conduct periodic conference calls to monitor the actions recommended by Supplier's respective teams or JPMC through completion.
    b. Ensure Supplier SMEs and senior management is made available to JPMC as needed.
    c. Provide periodic status update to JPMC Delivery Manager and to the JPMC Cyber Teams with which Supplier has been working.
4. Share relevant threat analysis (IP, IOCs, Forensic reports etc) with JPMC to ensure impact assessment.
5. Based on incident impact/severity, JPMC will determine additional actions to implement and any interim risk mitigation. For example, without limitation:
    a. Pull back/isolate data
    b. Shift temporarily to in-house/alternate provider
    c. Activate business continuity plan

Post Incident Response:

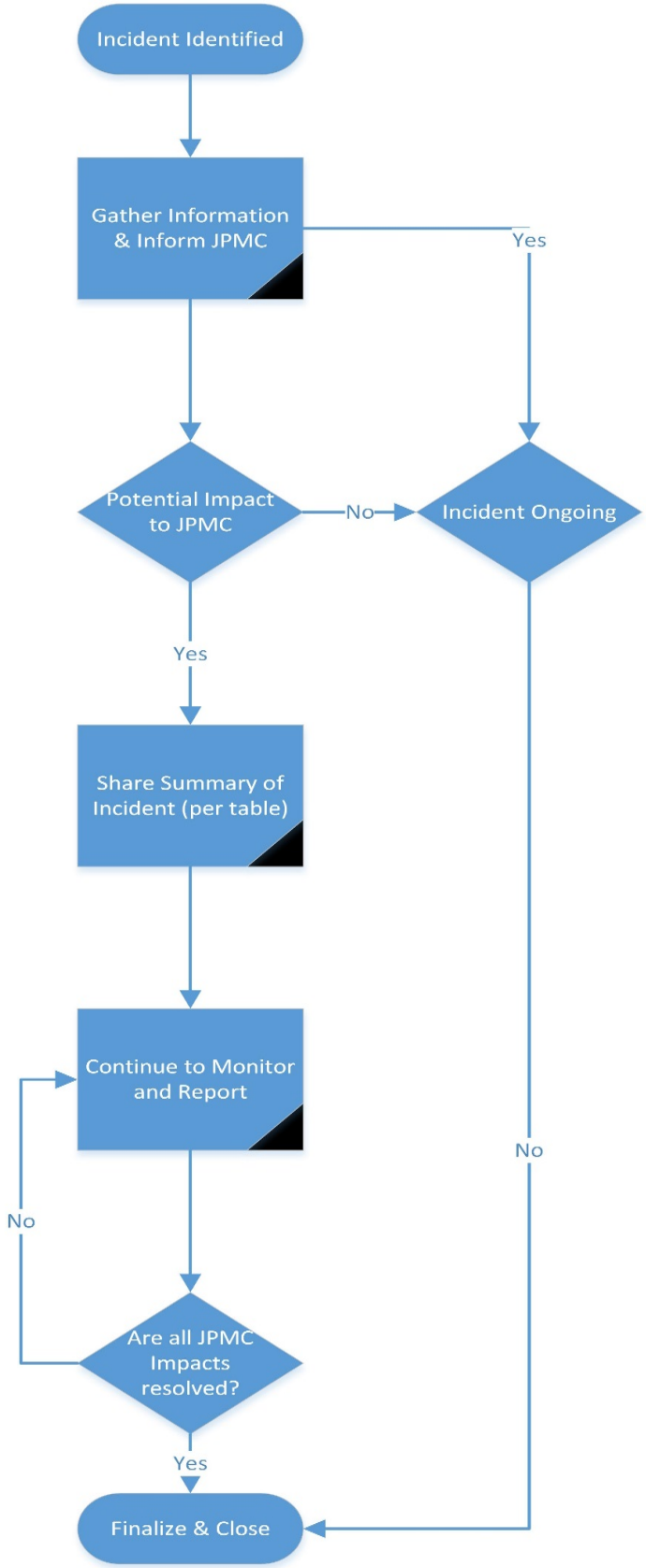
1. Discuss lessons learned and update controls where necessary.
2. Review and enhance Response Procedure runbook.
3. Store all incident response related documents for an adequate retention period as deemed appropriate period per legal and jurisdictional requirements.
4. Final report for distribution to JPMC stakeholders.

Incident Response Procedure – Best Practice Recommendations

Information Details JPMC will require:

Information	Description
Timing of Incident	What time did the incident occur?
Type of Incident	Virus, DDoS, ransomware, malicious attack , phishing, etc;
Nature of incident	A concise description of the identified incident and its potential JPMC impact (be as detailed as possible). In the event that data has been leaked or exfiltrated provide an indication of the extent of the data exposure and classification of data including JPMC impact.
Source of incident information	How was the breach discovered? For example, through notification from another party, from self-discovery, etc.
Investigation details	What actions have you taken as part of investigating the incident to confirm its potential scope and impact.
Remediation Activities	What actions are you taking (or have taken) to mitigate / remediate the incident? Have you engaged a 3rd party? Informed Legal authorities? Regulatory impact?
Impact Analysis	What is the JPMC impact analysis. For example, if there are any evidence in logs or the data that indicates unauthorized access to JPMC data.
Data Sharing	Are there audit logs? Indicators of Compromise (IOC)? Forensic reports?
Next Steps	What are your next steps? What's outstanding? Provide your timeline for full remediation and service restorations

Incident Response Procedure – Best Practice Recommendations



JPMC TPP WCAG STANDARD

JPMorgan Chase Bank, N.A. and/or one or more of its affiliates ("**JPMC**") has an agreement with a Third Party Provider (henceforth to be referred to as **"Supplier"**) for services and/or goods (the "**TPP Agreement**") that implicates this JPMC Third Party Provider WCAG Standard ("**Supplier WCAG Standard**").

In the event of a conflict between the TPP Agreement and this Supplier WCAG Standard, the TPP Agreement shall control. In the event a supplier identifies a conflict between the TPP Agreement and this Supplier WCAG Standard, the supplier shall promptly report such conflict in writing to the JPMC Relationship Manager of the TPP Agreement. Otherwise, the terms of the TPP Agreement shall be deemed consistent with this Supplier WCAG Standard.

Applicability

This Supplier WCAG Standard applies to a supplier where the supplier interacts with JPMC customers and/or employees via **digital content** offered through applicable JPMC web and mobile properties or by JPMC digital content delivered via supplier web and mobile properties, or as otherwise indicated by the TPP Agreement and/or JPMC Relationship Manager (or Delivery Manager as the case may be) as being applicable.

Conformance Requirements

1. The standard for accessible customer-facing and employee-facing digital content is the Web Content Accessibility Guidelines (WCAG) v2.1 Level A and AA success criteria established by the World Wide Web Consortium (W3C) and in compliance with the Twenty-First Century Communications and Video Accessibility Act.
2. All documents published in Portable Document Format (PDF) and accessed through digital channels must be **PDF/UA** conformant.
3. Without limiting the requirements of WCAG conformance generally, in the event the supplier does not conform to this Supplier WCAG Standard, supplier shall first obtain express written approval from the JPMC Relationship Manager confirming that such conformance variants have been approved by JPMC Risk and Controls.
4. To the extent supplier digital content requires remediation, such remediation will be completed in accordance with the following, unless otherwise agreed. The severity and priority of a defect will be determined by JPMC:
    a. Critical severity or critical priority defects for WCAG success criteria found prior to production release are to be remediated prior to production release
    b. Critical severity or critical priority defects for WCAG success criteria discovered in production must be remediated with the next production release or within 30 days, whichever is sooner
    c. High priority defects for WCAG success criteria are to be remediated within 120 calendar days after the defect was identified
    d. Medium and low priority defects for WCAG success criteria are to be remediated within 240 calendar days after the defect was identified
5. To the extent that the supplier identifies a WCAG defect in its digital content, supplier shall notify JPMC of each defect in writing within 15 days to allow for priority and severity assignment by JPMC.

Evidence Requirements

1. JPMC requires an Accessibility Conformance Report (ACR) in the form of a completed **Voluntary Product Accessibility Template (VPAT®)** as an indication of the supplier's product conformance either within 30 days of JPMC request and/or prior to production implementation of new or updated content that impacts user experience. The supplier may engage a third party, at their own expense, to perform an assessment and complete a VPAT®.

JPMC TPP WCAG STANDARD

2. JPMC may periodically conduct a review to assess the supplier's current accessibility maturity and ongoing conformance support capability. The expectation is that supplier provides response related to the review feedback within 30 days, unless otherwise agreed.
3. Related to applications used by JPMC employees, JPMC may perform accessibility assessments in our computing environment using a combination of automated, manual and assistive technology focused techniques.
    a. JPMC will provide the supplier with test results and a list of identified accessibility defects with assigned priority/severity classifications
    b. The supplier will provide an accessibility remediation roadmap outlining the target timeline to address the identified defects within 30 days of initial test results delivery or subsequent roadmap update request
        i. Remediation will be completed within a mutually agreed upon timeline not to exceed six (6) months, unless otherwise agreed.
    c. The supplier will provide updated remediation timelines and progress reports during recertification process

Definitions

1. "**Digital Content"** is text, images, sounds, videos and animations encountered as part of the user experience presented through various digital and electronic platforms and interfaces, including but not limited to websites, desktop or mobile applications, ATM interfaces, webinars, text messages, emails, electronic documents (such as PDFs) and plug-ins.
2. "**Voluntary Product Accessibility Template"** or "**VPAT®**" is a reporting format published by the Information Technology Industry Council (ITI) used to document a product's conformance with WCAG standards. The word "voluntary" within the title is not indicative that the VPAT® is an optional requirement.
3. **"PDF/UA"** is a Portable Document Format (PDF) built for Universal Accessibility (UA) in conformance with ISO 14289-1 standard which contains specifications for accessible PDF documents as published by the International Organization for Standardization (ISO).

Links

1. Web Content Accessibility Guidelines (WCAG) 2.1 standards are published by the Worldwide Web Consortium (W3C) at: https://www.w3.org/TR/WCAG21/.
2. The Voluntary Product Accessibility Template (VPAT®) is published by the Information Technology Industry Council (ITI) and can be downloaded from: https://www.itic.org/policy/accessibility.

JPMORGAN CHASE & CO.

Message from Ken Litton, Chief Procurement Officer and Rohan Amin, Global Chief Information Security Officer

Please read this important note and also ensure it is forwarded to any other accountable party for JPMorgan Chase at your organization.

As a third party supplier providing contingent workers to JPMorgan Chase, your firm plays a critical role in safeguarding JPMorgan Chase while creating industry leading technology and driving innovation. The nature of our work is often sensitive, proprietary, and highly confidential. As such, a simple job description posted on social media sites such as LinkedIn could give those outside JPMorgan Chase sensitive insights into what we do and how we do it.

Your firm has agreed to adhere to our Global Social Media Policy via the JPMorgan Chase Supplier Code of Conduct. The policy provides guidelines on the personal use of social media and reminds you and your contingent workers of the responsibility to protect JPMorgan Chase's confidential information and reputation at all times.

In accordance with this policy and effective immediately, JPMorgan Chase has enhanced guidelines pertaining to LinkedIn and other social media sites. Specifically, no information associated with JPMorgan Chase can be included in any contingent worker's LinkedIn or other social media profile while they are on assignment with JPMorgan Chase.

Please instruct all of your contingent workers providing services to JPMorgan Chase to ensure immediate compliance with this policy enhancement by removing any reference to JPMorgan Chase in their LinkedIn profiles (or other social media sites). JPMorgan Chase will be periodically monitoring these sites and a failure to adhere to these enhanced guidelines can result in JPMorgan Chase terminating any relevant agreements between our firms. Your continued provision of services to JPMorgan Chase shall represent your agreement with this notice.

If you have any questions, please click here.

Thank you in advance for giving this matter your immediate attention.

Supplier Minimum Control Requirements – 2022 Updates

December 2022

JPMorgan Chase & Co.

Supplier Minimum Control Requirements – 2022 Updates

Introduction

This change log references the JPMorgan Chase & Co. Minimum Control Requirements document (MCR), published in December of 2022. It specifies material changes made in this update cycle to facilitate comparison with the prior version. Use this change log as a guide and refer to the Minimum Control Requirements document itself for the exact wording of the controls.

Section 1: Holistic Changes to the Minimum Control Requirements

Supplier Minimum Control Requirements – 2022 Updates

Section 1: Holistic Changes

Subject of Change	Control Domain(s)	Description
None	N/A	• No changes to the structure/format/etc. of the Supplier Minimum Control Requirements for 2022

Section 2: Changes to Specific Control Domains

Supplier Minimum Control Requirements – 2022 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Subject of Change	Description
Technology Governance Risk and Compliance	• Change to 1 existing statement	• Security policies and responsibilities, including cybersecurity awareness training, must be communicated and socialized within the organization to Supplier Personnel.
Data Protection	• Addition of 3 new statements • Removal of 1 statement • Change to 2 existing statements	• Suppliers and dependent subcontractors must have sufficient information classification for the purpose of data protection • Data protection policy must be reviewed against industry standards on a regular basis. • Supplier must implement appropriate technical configuration for the protection of encrypted portable media. • ~~The ability to write to portable electronic media must be disabled where possible, and any exceptions must be documented~~ • All authentication credentials (e.g., passwords, personal identification numbers, challenge answers) must be encrypted in transit and at rest. • Supplier's data protection policy must cover ~~data classifications,~~ encryption ~~use~~, key and certificate lifecycle management, permitted cryptographic algorithms and associated key lengths, message authentication, hash functions, digital signatures, and random number generation ~~and be reviewed against industry standards on a regular basis.~~

Supplier Minimum Control Requirements – 2022 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Subject of Change	Description

Identity and Access Management	• Addition of 2 new statements
	• Removal of 1 statement
	• Change to 1 existing statement
		• A privileged account management process and control policy must be documented, covering privileged (system or elevated user) and non-privileged (personal) account separation, privileged account discovery, safeguarding of privileged accounts, post activity usage review requirements, and assurance that non-interactive privileged accounts (e.g., system accounts) are not used interactively by end users
		• Multi-factor authentication must be implemented for:
		  • The initiation of any interactive privileged access session ~~and/or retrieval of credentials with privileged access~~
		  • The administration of application access
		• ~~Management of privileged user accounts to include service accounts, must follow a documented process and be restricted.~~

Incident and Event Management	• Addition of 1 new statement • Removal of 1 statement • Change to 2 existing statements	• Documented incident, event, or problem management procedures must include systematic tracking ~~of problems~~ from discovery to resolution. • Supplier's event management policy and procedures must account for the ~~identification~~ detection, analysis, and presentation of anomalous events that indicate deviation from the norm beyond a defined threshold and engage JPMC via an incident management process. • ~~Supplier must also process and analyze events to determine if action is required, and to engage JPMC via the Incident Management process.~~ • Supplier's problem management policy must include documenting root cause analysis, implementation of permanent fix, preventative actions, and service improvement opportunities, providing conclusions to JPMC.

Supplier Minimum Control Requirements – 2022 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Subject of Change	Description
Security Configuration	• Change to 1 existing statement	• Network and host-based intrusion detection and/or intrusion prevention systems ~~(IDS and IPS)~~ must be deployed with generated events fed into centralized systems for analysis.
Security Operations	• Change to 1 existing statement	• Supplier Personnel must be trained to identify and report suspected security weaknesses, suspicious activity, and security events or incidents.
Technology Development	• Addition of 1 new statement • Addition to 1 existing statement	• Functional and non-functional requirements must be continuously identified and implemented to prevent software from becoming obsolete. • SDLC Governance must be established, documented, and enforced to identify and remediate defects, vulnerabilities, coding errors, and design flaws prior to production using a risk-based approach.
Technology Operations	• Removal of 2 statements • Addition of 3 new statements • Change to 3 existing statements	• See MCR Document for specific language
Privacy	• Addition of 1 new statement	• Supplier must have a process to notify JPMC of any event that may or will impact that confidentiality, integrity or availability of personal information, including unauthorized or suspicious intrusion into systems storing such personal information.

Supplier Minimum Control Requirements – 2022 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Subject of Change	Description
Data Risk Management	• Removal of 2 statements • Change to 6 existing statements	• See MCR Document for specific language
Organizational Security	• Change to 2 existing statements	• Supplier personnel assigned to JPMC Services must ~~be provided a copy of~~ review the JPMC Supplier Code of Conduct available at: https://www.jpmorganchase.com/about/suppliers • Supplier personnel must notify JPMC in the event of any potential~~, perceived~~ or actual conflicts of interest between Supplier personnel's outside business activities and personal relationships and JPMC business, clients, or employees.

Global Contingent Worker Pre-Engagement Screening (PES) Initiation Guide

Last Update: February 10, 2022

Copyright ©2021. All Rights Reserved. JPMorgan Chase Bank, N.A. Proprietary Information

Table of Contents

Copyright ©2021. All Rights Reserved. JPMorgan Chase Bank, N.A. Proprietary Information

Overview

This guide provides supplier instructions for initiating the JPMC Pre-Engagement Screening (PES) process in all regions for **Category 1 Contingent Workers**. PES is conducted by the JPMorgan Chase Global Workforce Screening (GWS) department.

PES must be conducted for all non-JPMC employees prior to starting an assignment. Any non-JPMC employee starting an assignment prior to clearance will be subject to immediate termination.

- **Category 1 (Contingent Worker):**
    - Requires ID Badge (unescorted access)
    - May require JPMC system access
- **Category 2 Supplier Personnel (NO ID BADGE REQUIRED)**:
    - No ID Badge (escorted access)
    - May require access to JPMC sensitive data
    - Reference the Vendor Initiation Guidefor specific guidance for Category 2 (vendor) screening
    - Category 2 Supplier Personnel are applicable in the United States only
- **Supplier Personnel Who Do Not Require an ID Badge / SID (EMEA Only)**
    - An individual who is not an employee and requires escorted access to a JPMC facility must complete **Permit Vetting** screening. For further information on the process, please contact emea.gws.helpdesk@jpmorgan.com.

Specific screening requirements and turn-around times will vary by country and are based on the JPMC work location.

Special Instructions

- Screening checks for Contingent Workers **cannot commence** until a Provisional SID has been issued by the CWOC Group.
- Screening must be initiated in the same region as listed Work Location.
- Individuals who have lived outside of country listed as work location within the past 5 years may be subject to additional screening checks.

Copyright ©2021. All Rights Reserved. JPMorgan Chase Bank, N.A. Proprietary Information

United States Pre-Engagement Screening Instructions

PES Pre-requisites:

- SID must be created or re-activated BEFORE initiating screening
- Applicant must use Legal name on screening applications
- Applicant must include SID and Cost Center when filling out screening application (provided by supplier)
- Applicant must include Personal E-mail Address on form (not supplier address) in case GWS is required to reach out to the candidate to obtain more information

Step 1: Create or re-activate SID

- Click here for further instructions on how to create an SID for onboarding contingent workers
  - Complete CWOC/CWP forms with Contingent Workers' full legal name
  - SID and Cost Center must be provided to Contingent Worker to complete their screening application

Step 2: Complete Demographic Profile (Background application):

- Supplier instructs candidate to visit **Application Station 2.0** to fill out demographic profile
- Enter code "**JPMCCW**" in the Application Station Code section
- Complete all required fields
- Submit application

Step 3: Schedule Fingerprint Appointment:

- Supplier instructs contingent worker to visit **Fieldprint** site.
- Contingent Worker creates an account by clicking "Schedule an Appointment"
- Once signed in, use the Fieldprint code "**FPCWCHASE**"
- Complete personal and demographic information
- Proceed to schedule your appointment

Screening results:

- JPMC will only disclose eligibility for assignment at JPMorgan Chase – no details of the screening results will be provided to the Supplier or Assignment Sponsor.
- The screening turn-around-time varies from 2 to 15 business days or more, depending upon factors such as personal data input, appointment scheduling and contingent worker's responsiveness to any requests for additional information.
- Individuals who have lived outside of the United States within the past 5 years may be subject to additional screening. Turn-Around-Time varies depending on the country where worker lived and could take up to 15-20 business days. Start dates must be planned accordingly.

Copyright ©2021. All Rights Reserved. JPMorgan Chase Bank, N.A. Proprietary Information

Canada Pre-Engagement Screening Instructions

PES Pre-requisites:

- SID must be created or re-activated BEFORE initiating screening
- Applicant must use Legal name on screening applications
- Applicant must include SID and Cost Center when filling out screening application
- Applicant must include Personal E-mail Address on form (not supplier address) in case GWS is required to reach out to the candidate to obtain more information

Step 1: Create or re-activate SID

- Click here for further instructions on how to create an SID for onboarding contingent workers
  - Complete CWOC/CWP forms with Contingent Workers' full legal name
  - SID and Cost Center must be provided to Contingent Worker to complete their screening application

Step 2: Initiate Screening:

- Supplier to provide candidate link to **Application Station 2.0**
- Enter code "**JPMCCANADA**" in the Application Station Code section
- Follow the below instructions:
  - Provide Standard ID (SID)
  - Provide Cost Center
  - Contingent Worker MUST use legal name
  - Contingent Worker MUST include Personal E-mail Address on form (not supplier address)
- Complete all required fields and submit application
- After submitting the application, Contingent Worker will receive a follow-up e-mail requesting additional required information

Screening results:

- JPMC will only disclose eligibility for assignment at JPMorgan Chase – no details of the screening results will be provided to the Supplier or Assignment Sponsor.
- The screening turn-around-time varies from 2 to 15 business days or more, depending upon factors such as personal data input, appointment scheduling and contingent worker's responsiveness to any requests for additional information.
- Individuals who have lived outside of the United States within the past 5 years will be subject to additional screening. Turn-Around-Time varies depending on the country where worker lived and could take up to 15-20 business days. Start dates must be planned accordingly.

Copyright ©2021. All Rights Reserved. JPMorgan Chase Bank, N.A. Proprietary Information

Europe/Middle-East/Africa (EMEA) Pre-Engagement Screening Instructions

PES is subject to local data privacy legal requirements and the relevant JPMC Privacy Notice, where applicable. Reference the Contingent Worker Permit Vetting Privacy Notice Here to understand how data is collected and what it is used for.

CONTINGENT WORKERS

Allow at least 25 business days for the completion of PES.

PES Pre-requisites:

- SID must be created or re-activated BEFORE initiating screening
- Applicant must use Legal name on screening applications
- Applicant must include SID and Cost Center when filling out screening application
- Applicant must include Personal E-mail Address on form (not supplier address) in case GWS is required to reach out to the candidate to obtain more information
- The UK Criminal Record Check for Contingent Workers in England/Wales requires the Supplier to view the Contingent Worker's **original** photograph ID (passport) and Proof of Current Address and provide attestation /upload a copy of the documents to the screening vendor before the check can be submitted.

Step 1: Create or re-activate SID

- Click here for further instructions on how to create an SID for onboarding contingent workers
  - Complete CWOC/CWP forms with Contingent Workers' full legal name

Step 2: Initiate Screening

- **Supplier SPOC** (Single Point of Contact) creates a new screening request on Enterprise Advantage or Vero Live
  - First time users need to set up an account and complete Case Requestor training - contact emea.gws.helpdesk@jpmorgan.com to be assigned the appropriate screening provider.
- **Screening Provider** sends log in details to the Contingent Worker via email, instructing them to complete their screening forms online.
- **Contingent Worker** submits their details in the online system following the instructions provided in the email from screening provider OR
- **Supplier SPOC collects details from Contingent Worker and submits Contingent Worker details on their behalf**
- **Screening Provider** will contact the Contingent Worker directly if additional information / documentation is required.
  - Individuals who have lived overseas within the past 5 years for six or more months will be subject to additional checks.
  - Additional specific Consent Forms may be required for checks in some countries in addition to the standard Consent Form.
  - Turn-Around-Time varies depending on the country and could take up to 15 – 25 business days; Turn-Around-Time for UK is typically 10 business days.

Copyright ©2021. All Rights Reserved. JPMorgan Chase Bank, N.A. Proprietary Information

Screening Results:

- JPMC will only disclose eligibility for assignment at JPMorgan Chase – no details of the screening results will be provided to the Supplier or AssignmentSponsor.
- Once overall clearance has been confirmed, the **Assignment Sponsor** will receive a "**Ready to Work**" email from CWOC.
- Start Date can be changed once "Ready to Work" email is issued

PERMIT VETTING

PES Pre-requisites:

- Permit Vetting applies to non-badged contractors only
- Suppliers required to use E-Permit for approval of works should obtain the E-Permit User ID prior to raising the screening request
- Applicant must use Legal name on screening applications
- The UK Criminal Record Check for Contingent Workers in England/Wales requires the Supplier to view the Contingent Worker's **original** photograph ID (passport) and Proof of Current Address and provide attestation /upload a copy of the documents to the screening vendor before the check can be submitted.

Step 1: Initiate Screening

- **Supplier SPOC** (Single Point of Contact) creates a new screening request on Enterprise Advantage or Vero Live
- First time users need to set up an account - contact emea.gws.helpdesk@jpmorgan.com to be assigned the appropriate screening provider.
- Suppliers required to use E-Permit should include the E-Permit User ID in the "LOB" field of the vendor request form
- **Screening Provider** sends log in details to the Permit Vetted Contractor via email, instructing them to complete their screening forms online OR
- Supplier SPOC collects details from Permit Vetted Contractor and submits Contingent Worker details on their behalf
- **Permit Vetted Contractor** submits their details in the online system following the instructions provided in the email from screening provider
- **Screening Provider** will contact the Permit Vetted Contractor directly if additional information / documentation is required.
    - Additional specific Consent Forms may be required for checks in some countries in addition to the standard Consent Form.
    - Turn-Around-Time varies depending on the country – contact emea.gws.helpdesk@jpmorgan.com for the current TATs by country
    - Turn-Around-Time for UK is typically 10 business days

Screening Results:

- JPMC will only disclose eligibility for assignment at JPMorgan Chase – no details of the screening results will be provided to the Supplier or AssignmentSponsor.

Copyright ©2021. All Rights Reserved. JPMorgan Chase Bank, N.A. Proprietary Information

Asia-Pacific (APAC) Pre-Engagement Screening Instructions

When submitting requests for security checks, please ensure requests are submitted well in advance of the start date (**allow at least 25 business days**), particularly for those with overseas address history. It is the **Supplier's** responsibility to confirm a contingent worker has authority to work in the relevant country. For **Suppliers** submitting requests for the first time, please contact **JPMC APAC GWS team** at asia.pes@jpmorgan.com to be assigned with one of JPMC's **Screening Providers** (First Advantage (FADV) or RISQ Group) and create an online account.

PES Pre-requisites:

- SID must be created or re-activated BEFORE initiating screening
- Applicant must use Legal name on screening applications
- Supplier must include all mandatory information i.e. SID, Cost Center, LOB details, etc when initiating a new screening request
- Applicant must include Personal E-mail Address on form (not supplier address) in case GWS is required to reach out to the candidate to obtain more information

Create or re-activate SID

- Click here for further instructions on how to create an SID for onboarding contingent workers
  - Complete CWOC/CWP forms with Contingent Workers' full legal name

Initiate Screening

- **Supplier** creates a new screening request on the assigned **Screening Provider's** online system.
- Log onto the system with your username and password.
  - FADV's EA system https://enterprise.fadv.com/ OR
  - RISQ's AMY system - https://global3.risqgroup.com/amya/Account/Login
- You will be taken to a Create Profile page.
- Create a new screening request either by using a '**Create Single Profile**' or '**Create Bulk Profiles**'.
- Complete all compulsory fields (marked with *).
- Click on '**Submit**' button.

- **Screening Provider** sends an email to the contingent worker, instructing them to complete their screening forms online. The email contains the username with instructions.

- **Contingent Worker** submits their details in the online system following the instructions provided in the email from Screening Provider.

- **Screening Provider** will contact the **Contingent Worker** directly if additional information/ documentation is required.
  - Individuals who have lived in an oversea address within the past 5 years for six or more months will be subject to additional screenings.
  - Additional Specific Consent Forms are required for checks in some countries in addition to the Standard Consent Form.
  - Turn-Around-Time varies depending on the country and could take up to 15 – 25 business days.

Copyright ©2021. All Rights Reserved. JPMorgan Chase Bank, N.A. Proprietary Information

Note: Screening process typically takes 15 – 25 business days **AFTER** the Contingent Worker has completed Step 3 and 4 above.

Screening results:

- JPMC will only disclose eligibility for assignment at JPMorgan Chase – no details of the screening results will be provided to the Supplier or AssignmentSponsor.
- Once overall clearance has been confirmed, the **Assignment Sponsor** will receive a '**Ready to Work**' email from CWOC.

Copyright ©2021. All Rights Reserved. JPMorgan Chase Bank, N.A. Proprietary Information

Latin America & Bahamas (LATAM) Pre-Engagement Screening Instructions

When submitting a security check request, please ensure they are requested well in advance of the start date, particularly for those with overseas address history.

1. **Supplier** completes the LATAM PES Request Form with all of the information requested:
    - Complete the details required. (Hire type, Name, DOB, SID, Cost Center, Start Date, etc.)
    - Type the email address for clarity. Provide a personal, not company, email address for the Contingent Worker.

2. **Supplier** scans and emails the completed LATAM PES Request Form at jpmc.latam.pes@jpmchase.com Please include in the email subject line:
    - Contingent Worker's name
    - Country
    - Company/Supplier name

3. **JPMC LATAM PES** initiates the screening process through BIG.

4. **BIG** sends an email to the Contingent Worker, instructing them to complete their screening forms online.

    - **Note: Supplier** should confirm with the Contingent Worker that they received this BIG (applicationstation@bigreport.com) E-mail within 48 hours of when the supplier submitted the LATAM PES Request Form. If the Contingent Worker doesn't see the email, first have them check their spam folder and filters. If the email is not there, please contact jpmc.latam.pes@jpmchase.com

5. **Contingent Worker** submits the required data online using the BIG system following the instructions provided in the email from BIG (applicationstation@bigreport.com)
6. **JPMC Global Security & Investigations** will contact **Supplier** if there are issues or if additional information/documentation is required.

7. Once overall clearance has been confirmed, the **Assignment Sponsor** will receive a '**Ready to Work**' email from CWOC.

Note: The screening process typically takes 5-10 business days AFTER the Contingent Worker has completed step 5 above.

Screening results:

- JPMC will only disclose eligibility for assignment at JPMorgan Chase – no details of the screening results will be provided to the Supplier or AssignmentSponsor.

Copyright ©2021. All Rights Reserved. JPMorgan Chase Bank, N.A. Proprietary Information

Instrucciones para Pre-Engagement Screening en Latinoamerica & Bahamas (LATAM)

Cuando se solicita una verificación, por favor asegurarse que es solicitada correctamente y con anticipación a la fecha de inicio, particularmente para aquellos que tienen un historial de direcciones en el extranjero.

1. **El Proveedor** completa el LATAM PES Request Form con toda la información requerida:
    - Detalles completos requeridos. (Tipo de contratación, Nombre, Fecha de nacimiento, SID, Centro de Costos, Fecha de Inicio, etc)
    - Escribir el e-mail con claridad. Proveer un mail personal, no de la compañía, para el trabajador.

2. **El Proveedor** escanea y envía por mail el LATAM PES Request Form completo a jpmc.latam.pes@jpmchase.com
   Por favor incluir en el asunto del mail:
    - El nombre del trabajador
    - País
    - Compañía / Proveedor

3. **JPMC LATAM PES** inicia el proceso de verificación a través de BIG (Vertical Screen)

4. **BIG** envía un mail al trabajador, instruyéndolo para completar su formulario de screening on line.
    - **Nota: El proveedor** debe confirmar con el trabajador que haya recibido el email de FBIG dentro de las 48hs desde que el proveedor envió el formulario LATAM PES Request Form. Si el trabajador no ve el email, primero debe chequear su carpeta de correo no deseado. Si el mail no está allí entonces, por favor contactarse con jpmc.latam.pes@jpmchase.com

5. **El Trabajador** envía la información solicitada online usando el sistema de BIG siguiendo las instrucciones provistas en el mail de BIG (applicationstation@bigreport.com)

6. **JPMC Global Security & Investigations** notificará al **proveedor** si hay algún inconveniente o si se necesita información/documentación adicional.

7. **CWOC** enviará un mail al Assignment Sponsor confirmando que el proceso de PES fue terminado (*ready to work* email)

   Nota: El proceso normalmente lleva 5-10 días hábiles después de que el trabajador haya completado el paso 5to arriba mencionado.

   Resultados del screening:
    - JPMC sólo revela la elegibilidad para el trabajo en JPMorgan Chase – ningún otro detalle va a ser provisto.

Copyright ©2021. All Rights Reserved. JPMorgan Chase Bank, N.A. Proprietary Information

Systems Monitoring

Purpose

The following describes the practices of JPMorgan Chase & Co., its affiliates and its subsidiaries and the entity that employs you, or for which you provide services (collectively, "JPMC"), with respect to the monitoring of JPMC's physical facilities, equipment and systems (collectively, the "Systems"). These Systems are provided for work-related purposes and monitoring is designed to protect the Systems and your use of the Systems. JPMC monitors the Systems to protect you, your colleagues, the firm, and others as described when you log into your workstation, in our Supplier Code of Conduct, and in this document.

Scope and Application

Systems monitoring applies to JPMC employees or other persons who use JPMC's equipment and systems in the context of an employment or other working relationship with JPMC (collectively, "Workers"). Some Workers may be more frequently monitored than others due to the nature of their work, including registered and licensed personnel and traders (regulated workers). The Systems include business equipment and electronic communications tools, such as servers, terminals, computers, databases, applications, telephones, mobile and portable devices, fax and copy machines, printers, internet, email, instant messaging platforms, and voicemail. Systems monitoring applies to your JPMC equipment, your personal equipment when accessing the Systems, and the communications, information, and materials conveyed or accessed using the Systems.

Monitoring Activities

JPMC may conduct monitoring as described in this document, and in additional notices that may be provided to you, subject to applicable laws and regulations. JPMC's monitoring activities may include:

- monitoring and logging of (1) traffic and usage data (such as routing, addressing, or signaling information, time and date stamps, sender and recipient details and file size) related to incoming, outgoing and internal electronic communications, including emails sent to and from JPMC accounts, chats and instant messages on JPMC-approved channels for business use (such as Bloomberg messages), and any other data moving across the Systems (including internet traffic); and (2) Systems activity, including files or information accessed or downloaded from, or uploaded to Systems;
- monitoring contents of (1) emails sent to and from JPMC accounts; (2) chats and instant messages on JPMC-approved channels for business use; (3) faxes sent to or from JPMC fax numbers; (4) text messages (SMS) sent to or from Systems; (5) files or information accessed or downloaded from, or uploaded to Systems; and (6) internet usage (including pages visited and searches made) (collectively, the "Content");
- monitoring telephone calls to or from JPMC work telephones as required or permitted by applicable laws and subject to any required notices;
- capturing Workers' physical presence at JPMC's facilities via for example access badges and video cameras, which record activities at exits, entrances, corridors, and other public areas; and
- logging hours worked if applicable to the Worker.

To the extent permitted by applicable law, JPMC may at all times monitor, access, retrieve, record, and review information obtained via monitoring activities, including any Content, and any personal use of the Systems, as reasonably necessary or advisable in JPMC's interests for purposes including:

- preventing and investigating activities that could violate JPMC's policies or applicable laws, such as market abuse, financial crimes, bank regulatory and reporting violations, improper product marketing, mis-selling, trade violations, Code of Conduct violations, or misuse or inappropriate sharing of information;

- detecting, blocking, and flagging offensive terms or Content on the Systems; access to inappropriate or unauthorized websites or IP addresses; and unauthorized transmissions of confidential, proprietary, or sensitive information;
- finding lost or deleted messages;
- auditing and conducting other internal analyses;
- complying with legal or regulatory obligations; and
- protecting the security of JPMC's Systems or other assets, including flagging potential misuse of the Systems and detecting viruses and malicious software and unauthorized access.

Monitoring activities may be conducted (1) by automated means, sampling or manual reviews; and (2) routinely or in connection with specific incidents, investigations, or inquiries from human resources or other departments. Subject to applicable laws and regulations, information obtained from the monitoring activities may be used as the basis to take disciplinary actions, up to and including termination or other legal action, for violations of JPMC's policies or applicable laws.

Personal Information

While conducting monitoring activities, JPMC may obtain and process personal information about you and others, including names, email addresses, home addresses, account information, and other personal information, that may reside on the Systems. JPMC takes steps to process the minimum personal information necessary when conducting monitoring activities. To the extent permitted by applicable law, the monitoring activities are required to promote adherence to applicable policies and regulations.

Disclosures

As permitted or required by law and for the purposes noted above, JPMC may disclose Content or other information obtained in connection with monitoring activities to JPMC affiliates or to third parties, service providers, regulators, supervisory bodies, law enforcement, or other government agencies. JPMC and its affiliates may jointly use any information collected in connection with monitoring activities for the purposes described here.

Cross-Border Data Transfers

JPMC may transfer the information it obtains in connection with monitoring activities to countries other than the country in which the information originally was collected, including to the United States, subject to applicable laws and regulations.

Retention

JPMC may retain the information obtained in connection with the monitoring activities for as long as (1) necessary to accomplish the purposes for which the information was collected or (2) the information is stored for legal or regulatory purposes such as regarding regulated workers.

Rights of Workers

This document describes any rights you may have, including rights to access and correct information JPMC obtains about you, in accordance with established procedures in your country. Please direct any questions you may have to your JPMC assignment sponsor.

Supplier Environmental Sustainability Guidelines

Updated January 2023

I. Introduction

JPMorgan Chase & Co. ("JPMC", the "Firm" or "we") believes that responsible and sustainable business practices are important to the long-term interests and stability of the Firm and its clients, customers and other stakeholders. To support and advance our Firm's commitment to sustainability, including our goal of achieving and maintaining carbon neutrality across our operations, we are enhancing our sustainability strategy to consider the policies and practices of our suppliers.

These Supplier Environmental Sustainability Guidelines ("Guidelines") are intended to establish a framework for our Firm to further incorporate environmental considerations into our procurement process, and to encourage JPMC suppliers to integrate positive environmental practices within their own organizations. The Guidelines are also intended to assist suppliers in preparing for compliance with future mandatory standards, including those that may be required by regulators, JPMC and/or their other customers.

II. Establish and Report on Sustainability Goals and Policies

Developing and implementing robust environmental policies and practices, and reporting on progress, is central to managing organizations' key environmental impacts, risks and opportunities, and to being publicly accountable for their performance. Key recommendations:

- **Implement and report environmental policies and practices.** JPMC encourages suppliers to implement and report on their short-term and long-term efforts to address environmental impacts, including but not limited to reducing GHG emissions, increasing energy efficiency, reducing water consumption and increasing waste diversion from landfills. Reporting may be submitted directly to JPMC or into any third-party supplier sustainability platform that JPMC may select to manage such data collection.
- **Set public goals to reduce environmental impacts.** JPMC encourages suppliers to publish public goals to reduce the environmental impact of their operations, products and services – including science-based climate targets, such as GHG emissions reduction or percentage of renewable energy – and to publicly report progress relative to these goals. JPMC further requests suppliers' cooperation in contributing such information to any sustainability platform that we may select to manage reporting for our supply chain.
- **Manage own supply chain.** JPMC encourages suppliers to establish similar expectations for their first-tier suppliers to set long-term environmental sustainability goals and to review second-tier suppliers as part of their overall sustainability strategies.

III. Measure and Disclose Key Environmental Impacts

Measuring and disclosing key environmental impacts – such as energy and water consumption, greenhouse gas (GHG) emissions, waste, air and water pollution, erosion and hazardous materials – helps organizations identify related risks and opportunities, design and implement more effective environmental policies and practices, and track their progress over time. Key recommendations:

- **Calculate and disclose GHG footprint.** JPMC encourages suppliers to calculate and disclose their GHG footprint, including both direct and indirect emissions and related climate impacts, in accordance with standard GHG accounting protocols. JPMC further requests suppliers' cooperation in providing this information to support calculation of GHG emissions in our supply chain.
- **Evaluate and mitigate climate change risks.** JPMC encourages suppliers to evaluate the potential adverse impacts of climate change on their operations and the related potential financial impacts to their businesses, and to disclose their findings. Suppliers are further encouraged to actively mitigate those risks to minimize the potential impact to their operations and potential impacts to JPMC.

IV. Promote a Culture of Environmental Sustainability

Promoting a culture of environmental sustainability and corporate responsibility is important for the successful integration and continuous improvement of related policies and practices. Key recommendations:

- **Train employees on environmental sustainability.** JPMC encourages suppliers to implement programs to train current employees and new hires on their companies' sustainability policies and practices.
- **Establish oversight and management of environmental sustainability.** JPMC encourages suppliers to establish clear structures for oversight and management of their sustainability programs and to hold senior leaders accountable for their programs' success.

JPMorgan Chase & Co. Supplier Code of Conduct

1. Summary

JPMorgan Chase & Co. and its subsidiaries (collectively referred to as JPMorgan Chase or the firm) are committed to building and maintaining the best and most respected financial services company in the world. As our business partners, Suppliers likewise have a duty to demonstrate the highest standards of ethical business conduct, integrity, and adherence to the law, at all times. The firm is committed to ensuring Suppliers act with honesty and integrity when acting on our behalf. This commitment to ethical business practices preserves our firm's integrity and reputation and fosters a safe, healthy, productive, and collaborative work environment.

The Supplier Code of Conduct (Supplier Code) sets out expectations for Suppliers and outlines the principles that are consistent with the regulatory and legal framework that governs our industry. It is the responsibility of Suppliers to know the requirements of the Supplier Code and operate in accordance with its principles. Suppliers must be aware of the Supplier Code's provisions and stay informed of any changes. The most current version is available online and effective when posted.

The Supplier Code does not constitute an employment contract, and nothing contained herein is intended to convey any rights, actions, or remedies to Suppliers, or to create an employment relationship between Supplier or Supplier's employees and the firm.

2. Scope

A ***Supplier*** is any third party, firm or individual that provides a product or service to JPMorgan Chase. The following persons, entities, and organizations (collectively referred to as Suppliers) are covered by the Supplier Code and thereby subject to its provisions:

- Suppliers, vendors, consultants, agents, contractors, temporary workers, and third parties working on behalf of the firm; and
- The owners, officers, directors, employees, consultants, affiliates, contractors and subcontractors of these organizations and entities.

3. Updates from Previous Version

- The Summary section was updated to highlight the importance of ethical conduct.
- Compliance with the legal and regulatory requirements were combined into a single section. Additional information related to assisting the firm in meeting its legal and regulatory obligations was incorporated in this section.
- A separate section on Reporting Concerns was created. References to the Code Reporting Hotline were replaced with the JPMC Conduct Hotline.
- Cryptocurrency and other digital assets were added as examples of prohibited gifts.
- The Human Rights section was updated to clarify Suppliers' obligations to ensure that their workforce meets the minimum legal age requirements for employment.

4. JPMorgan Chase Business Principles

The firm believes that certain Business Principles are fundamental to success. These principles include a commitment to exceptional client service, operational excellence, integrity, fairness, responsibility, and a winning culture. They describe how the firm conducts business and the type of culture we expect our Suppliers to foster.

5. Complying with the Legal and Regulatory Requirements

The Supplier Code must be read in conjunction with any applicable statutory, regulatory, or other legal obligation, including the contractual arrangements Suppliers have with the firm. Suppliers must comply with all applicable statutory, regulatory, or other legal obligations in the countries in which the Supplier operates.

Suppliers are expected to provide reasonable assistance to JPMorgan Chase so the firm can meet applicable legal and regulatory requirements in the countries in which we do business. This includes cooperating with regulatory inquiries and investigations related to outsourced services. Suppliers are also expected to cooperate with regulators in continuing to perform contracts, if required.

If compliance with any provision of the Supplier Code would result in a violation of statutory, regulatory, or other legal obligations, Suppliers must follow the legal obligation. Where the Supplier Code a contractual agreement with the Supplier conflict, the contractual agreement with the Supplier prevails.

For more information on the applicable firm policies and procedures referenced herein, Suppliers should contact their JPMorgan Chase ***Relationship Manager***.

5.1. Maintaining Policies to Ensure Compliance

Suppliers must conduct their operations in accordance with this Supplier Code and must have policies and procedures designed to ensure compliance with it, including but not limited to appropriate non-discrimination and non-retaliation policies. Suppliers must also make reasonable efforts to train, monitor, and ensure that their own supply chain is compliant with the Supplier Code and all contractual obligations.

5.2. Handling Information Properly

JPMorgan Chase is part of a highly regulated industry and all of the parties with which we have relationships, with including our customers and employees, expect us to safeguard their information. Suppliers must understand and comply with any applicable requirements and restrictions related to the processing of information including material, non-public information (MNPI). The processing of information means any operation or set of operations that is performed on information, whether automated or manual, including, but not limited to: collecting, recording, accessing, organizing, storing, adapting, altering, retrieving, consulting, using, disclosing, analyzing, transmitting, disseminating, aligning, combining, blocking, erasing, or destroying information. The following provisions regarding the processing of information survive the termination of the Supplier's provision of services to the firm, and the Supplier remains liable for any unauthorized processing of information belonging to the firm.

5.2.1. Confidentiality

Suppliers have a duty to protect ***confidential information*** and to take precautions before sharing with anyone. Suppliers are expected to comply with all applicable statutory, regulatory, or other legal obligations governing the protection or the processing of firm proprietary, confidential and ***personal information***. Suppliers may only process confidential firm information to perform work on behalf of JPMorgan Chase and may not disclose such information unless such disclosure is required by law. Suppliers must safeguard the confidential information of third parties, including anything that Suppliers learn or create while providing services to the firm and its customers and employees.

5.2.2. Privacy

Suppliers must be aware of and follow the applicable statutory, regulatory, or other legal obligations related to the processing of any individual's personal information pursuant to their relationship with JPMorgan Chase. Personal information must never be processed in a manner inconsistent with the terms of the Supplier's contractual arrangements with the firm, accessed by the Supplier or its employees without appropriate authorization, or disclosed to anyone outside of the firm or the Supplier, except as required by a legal or regulatory process and as permitted by the Supplier's contractual arrangements.

If there is any event that impacts, or may impact the confidentiality, integrity or availability of personal information, including unauthorized or suspicious intrusion into systems storing such personal information, Suppliers must immediately report such incident to their Relationship Manager in accordance with the terms of its agreement with JPMorgan Chase.

5.2.3. Material Non-Public Information

Material Non-Public Information (MNPI), also known as inside information, is information about an issuer of financial instruments (JPMorgan Chase or another) that is not known by the public but if it were, would likely: (1) affect the market price of the financial instruments to which the information relates; (2) influence a reasonable investor to trade those financial instruments; or (3) be used as part of an investment decision regarding those financial instruments.

Buying or selling securities while in possession of MNPI that is acquired by virtue of Supplier's relationship with the firm is strictly prohibited, as is the communication of that information to others, whether expressly or by making a recommendation for the purchase or sale of securities based upon that information.

MNPI must be safeguarded and should only be shared with those who have a business need for knowing the information. Need-to-know is where such information is necessary to carry out one's job responsibilities and the sharing is in connection with fulfilling those responsibilities to the firm.

5.3. Conflicts of Interest

Conflicts of interest affect objectivity when making decisions on behalf of the firm, and may be impermissible as a matter of law, regulation, or firm policy. The existence of potential and actual conflicts may also undermine credibility and impair good judgment.

A conflict of interest may exist when the interests of a Supplier oppose the interests of the firm or its clients. Personal or business relationships, outside interests and other external activities and personal investments, the exchange of gifts and business hospitality, and

political engagement can all pose potential conflicts. To identify and manage such conflicts, Suppliers must disclose all actual, perceived, or potential conflicts of interest with JPMorgan Chase as a result of either:

- Personal or business relationships with firm customers, suppliers, business associates, and employees with whom they work and/or support; and
- Outside interests related to the Supplier's role and responsibilities at JPMorgan Chase

All potential conflicts of interest must be reported to the Supplier's Relationship Manager at the firm or escalated to the Supplier personnel responsible for reporting such matters to the firm.

5.4. Doing Business Properly

JPMorgan Chase works to achieve a competitive advantage through the products and services we offer, not through unethical or illegal business practices or the appearance of such activities.

5.4.1. Bribery and Anti-Corruption

The firm does not tolerate bribery or corruption in any form. Suppliers and those acting on their behalf may not directly or indirectly offer, promise, authorize, recommend, give, solicit, or receive anything of value, if it is intended, or could reasonably appear as intended to influence improper action or to obtain or retain an improper advantage for the firm, the Supplier, or a third party.

- Anything of value may include ***gifts*** (including cash and cash equivalents), business hospitality (including accommodations, travel and related expenses, meals, and entertainment), training and conferences, contributions to a charitable or political organization on behalf of another, honoraria and speaker fees, visa letters, offers of employment or other work experience - whether paid or unpaid, secondments, sponsorships, raffle prizes, perks, or discounts.

Suppliers and those acting on behalf of Suppliers are prohibited from providing a facilitating or expediting payment, usually a small amount of currency or other item or instrument of value, to any government official for his or her personal benefit to cause the official to perform, or to expedite performance of a routine duty or function that the official is required to perform (e.g., a payment to get through customs or to obtain a permit quickly).

Suppliers are also responsible for knowing and complying with the anti-corruption and bribery laws in the jurisdictions in which the Supplier operates. Suppliers must promptly report any potential or actual violations that relate to the firm through either the JPMC Conduct Hotline or to their Relationship Manager.

5.4.2. Gifts

The provision of ***gifts*** can be misinterpreted, suggest the appearance of an improper exchange or cause one to compromise their integrity. Therefore, suppliers are not permitted to provide or offer any gift that may create an actual or potential conflict of interest, impair one's judgment, is intended or could be interpreted as intended to improperly influence decision-making. Gifts given for the benefit of JPMC employees or their family members, or to JPMC clients or business partners are discouraged and only permissible under the following circumstances:

- Meals, refreshments, and entertainment offered during the course of a meeting as long as the purpose is business-related, attendance relates to the employee's work, the Supplier is in attendance, the cost is reasonable and customary, and it is an infrequent occasion;
- Advertising and promotional materials of de minimis value; or
- Discounts and rebates offered to the general public or negotiated with the firm.

5.4.3. Political Activities and Lobbying

Suppliers must not make ***political contributions*** or provide ***gifts*** to any candidate for public office, elected officials, political parties, or committees on behalf of or as a representative of the firm. Suppliers must not represent their political views as those of the firm or use firm resources in connection with their political activity. Suppliers must not ***lobby*** on behalf of the firm unless specifically engaged in writing to do so.

5.4.4. Antitrust and Competition Laws

Antitrust and competition regulations prohibit anticompetitive or collusive agreements among competitors, including price-fixing, bid rigging, allocation agreements, and group boycotts. These regulations also prohibit predatory and exclusionary conduct by firms that have market power or a dominant position that is intended to lessen competition.

Suppliers are required to be aware of and comply with these antitrust and competition regulations when conducting business with or on behalf of the firm. Suppliers must also refuse to participate in any potentially anticompetitive behavior or inappropriate discussions with competitors such as those relating to pricing, bids, or bidding strategies and must report any such activity related to the firm to their Relationship Manager or through the JPMC Conduct Hotline.

5.4.5. Taxes

JPMorgan Chase is committed to complying with both the letter and the spirit of applicable tax laws wherever we operate and ensuring accuracy in the tax-related records we produce and the tax information we are required to report. Suppliers must not facilitate any activities by clients or other parties associated with the firm that are intended to breach applicable tax laws, which may include engaging in activities that would assist in evading the payment of taxes that are due and payable or concealing information from tax authorities.

Suppliers should adopt reasonable prevention procedures and be alert to all unusual or suspicious activities that may have as their purpose or apparent purpose hiding income or assets from tax authorities or evading the application of tax reporting requirements. Suppliers must promptly report any violations or suspected violations that relate to the firm through either the JPMC Conduct Hotline or to their Relationship Manager.

5.5. Workplace Environment

JPMorgan Chase believes in a positive, safe, and healthy workplace environment which fosters respect and inclusiveness among workforce members.

5.5.1. Non-Discrimination, Non-Retaliation and Diversity

The firm encourages an inclusive and supportive working environment free from harassment and intimidation, where all workforce members are valued and empowered to succeed.

Suppliers must comply with all applicable laws relating to discrimination in hiring, employment practices, harassment, and retaliation, including those that may apply as a result of the firm's contracts with government entities.

The firm actively encourages Suppliers to embrace diversity in their own business practices by documenting a diversity and inclusion approach that includes ways to identify, measure and improve inclusion and embedding accessibility standards that go beyond minimum compliance.

5.5.2. Working Conditions, Health and Safety

Suppliers must comply with all applicable firm policies, as well as safety and health laws and regulations in the jurisdictions where they operate. Suppliers must comply with all labor laws and employ only workers who meet applicable minimum age requirements in the jurisdiction. Suppliers must also comply with all applicable wage and hour labor laws and regulations governing employee compensation, reimbursements, taxes, and working hours.

Suppliers must provide a work environment free of threats, intimidation, and physical harm that supports accident prevention and minimizes exposure to health risks.

6. Raising Conduct Concerns

Suppliers must promptly notify the firm, if permitted by law, regarding the receipt of any subpoenas, regulatory requests, media inquiries, or other third-party requests concerning JPMorgan Chase.

The firm requires prompt, accurate, and transparent reporting of any conduct concern or actual or suspected violation of any law or regulation related to firm business, the Supplier Code, or any firm policy, including those addressing fraud, dishonesty, and unfair or unethical conduct related to financial services, whether it is by Supplier's team, a firm employee, or another third-party supplier. Concerns can be raised by contacting the Relationship Manager or using the Code Reporting Hotline (1-855-JPMCODE (1-855-576-2633)). Suppliers can also file a report online at www.tnwgrc.com/jpmc. Where permitted by law, Suppliers may report anonymously.

Failure to report a concern or violation may result in the termination of the Supplier relationship and applicable agreements.

The firm strictly prohibits intimidation or retaliation against anyone who makes a good faith report about a potential or actual violation of the Supplier Code, supporting policies, or any law or regulation.

Nothing in this Section or the Supplier Code is intended to require reporting in violation of applicable local law or regulation.

7. JPMorgan Chase Rights

JPMorgan Chase reserves the following rights to properly monitor and address Supplier activity to ensure that the firm is meeting its legal and regulatory requirements and obligations.

7.1. Firm Monitoring and Right to Audit

The firm reserves the right to monitor, record, review, access and disclose all data and communications created, sent, received, stored, or downloaded using firm resources as it deems appropriate, subject to applicable laws and regulations.

The firm also retains the right to audit Supplier compliance with the Supplier Code and other firm policies at any time. This includes technical, legal, regulatory, financial and operational audit of Supplier policies and procedures, including subcontractors if necessary, and in some cases may require an on-site inspection of Supplier's books, records, systems, controls, processes and procedures related to the JPMorgan Chase engagement for adherence to the Supplier Code.

7.2. Termination and Indemnification

The firm may take all necessary actions to enforce the Supplier Code, including the termination of Supplier relationship and applicable agreements. Violations of the Supplier Code may also constitute violations of law, which may expose the firm to criminal or civil penalties. The firm may require reimbursement for any costs associated with a violation of the Supplier Code.

8. Supplier Obligations to JPMorgan Chase

Suppliers must follow the obligations and requirements set forth below. By doing so, Suppliers will help the firm meet its legal and regulatory requirements, protect firm assets, and ensure that all communications are accurate and appropriate.

8.1. Communications about or on behalf of JPMorgan Chase

Suppliers must not communicate publicly about firm business unless specifically authorized to do so. Suppliers may not make public announcements on the provision of goods or services to the firm, share information regarding firm assignments, or circulate pictures or descriptions of firm facilities or external work events. Suppliers may not share information regarding firm customers or employees unless it is in connection with the services being provided as set forth in Supplier's agreement.

Suppliers must not post, share or like anything that could be viewed as a violation of the Supplier Code, including items that are malicious, disparaging, bullying, or that could jeopardize the safety of another individual including but not limited to firm employees, clients, or other Suppliers.

Suppliers should not disclose confidential information or conduct surveys of or post or seek recommendations or referrals by firm employees, customers or service providers unless approved. Exercise caution when discussing any of the firm's brands, products, services, or programs on social media. Suppliers are not encouraged or required to promote JPMorgan Chase.

8.2. Protecting IP and other Firm Assets

Suppliers must properly safeguard and protect ***firm assets*** from theft, waste, cyber-related attack, or other type of loss. Technology assets, office equipment and supplies, email systems, information assets such as intellectual property, and firm brand and customer relationships are the property of the firm and should be used for firm-related business

purposes only. Unless otherwise agreed to by the firm, any invention, discovery, development, concept, idea, process, or work related to the firm's business belongs to the firm and is considered work made for hire or ***company invention***.

Suppliers must have programs in place that meet or exceed the firm's Minimum Control Requirements designed to protect firm information. Never forward firm information to an external email address for any non-business purpose or to Supplier or Supplier employees' personal email accounts for any reason.

8.3. Accurate Records

Suppliers are responsible for maintaining accurate and complete books and records and complying with all required controls and procedures for records created as a result of business activities conducted on behalf of the firm. Suppliers must be aware of and comply with the legal and regulatory retention requirements that relate to the services being provided to the firm.

8.4. Knowing your Workforce Members

Suppliers are required to screen their workforce members (employees and contingent workers) who provide services to the firm in accordance with firm requirements before and during the engagement with JPMorgan Chase.

The Supplier must have reporting requirements for the Supplier's personnel performing work for the JPMorgan Chase engagement if they are involved in a criminal proceeding or other legal matter. With the exception of minor traffic violations/citations, all of the Supplier's personnel performing work on the engagement must promptly notify the Supplier regarding any current arrest and/or pending criminal charges and provide supporting documentation related to the matter. The Supplier must promptly notify JPMorgan Chase if any of the Supplier's personnel performing work on the engagement report an arrest or has pending charges.

9. Environmental and Social Sustainability, Human Rights

JPMorgan Chase recognizes that our business decisions have the potential to impact surrounding communities and the environment. Balancing environmental and human rights issues with our business are fundamental.

9.1. Environmental and Social Sustainability

The environmental and social commitment at JPMorgan Chase is integral to good business practices. The firm encourages and relies upon Suppliers to join us in that commitment by developing internal programs designed to foster a culture of sustainability across their own operations and supply chain. That includes setting environmental and social targets, preventing, mitigating, or ending adverse impacts, and reporting on progress.

Suppliers must comply with all applicable firm policies, environmental laws, and regulations in the countries in which the Supplier operates and in countries where they provide products or services. Suppliers should conduct operations in a manner that protects the environment by making reasonable efforts to meet industry best practices and standards with respect to the reduction of energy use, greenhouse gas emissions, waste, and water use. Suppliers must also ensure that potential impacts to community health, safety, and security – such as

accidents, impacts on natural resources, exposure to pollution or other community issues – that may arise from business operations are appropriately, prevented, mitigated, and managed.

As JPMorgan Chase refines its understanding of how sustainability impacts business, the firm is relying upon Suppliers to promote environmental and social stewardship and highlight opportunities to improve our understanding and management.

9.2. Human Rights

JPMorgan Chase is dedicated to upholding and protecting human rights around the world. It is the firm's responsibility to promote respect for human rights through actions, and the firm expects the same of Suppliers. The firm is guided in this effort by the principles set forth in the United Nations Universal Declaration of Human Rights.

The firm expects Suppliers to take all necessary steps to ensure that it does not employ anyone under the minimum legal age for employment. In addition, the firm expects Suppliers to adhere to human rights laws by working to prevent forced labor and human trafficking in their operations and supply chains, and by instituting practices that are consistent with the framework provided by the Guiding Principles on Business and Human Rights, as well as rights and prohibitions included in other international human rights agreements.

10. Defined Terms

Company Invention	Any Invention, discovery, development, concept, idea, process, or work, whether or not it can be considered a trade secret, patented, trademarked or copyrighted, that is directly or indirectly related to JPMorgan Chase business which Supplier develops during the period that Supplier works for JPMorgan Chase. This includes any invention unrelated to JPMorgan Chase business that is developed on firm time or with the use of firm equipment, supplies, or facilities.
Confidential Information	Information the firm has or acquires that is kept private and not made available to the public. It includes personal information about firm employees, customers and non-public information about clients and partners and their business. Any information that is not readily available from a public source or is shared between parties in confidence should be treated as confidential.
Conflicts of Interest	Supplier's personal and/or outside business interests may create potential or actual conflicts with the firm. This includes personal relationships or business opportunities with firm clients and potential clients, employees, and other suppliers. **Personal relationships** include family members such as a partner or spouse, children, siblings, parents or grandparents. **Business opportunities** include affiliation with (as director, officer, board member, etc.) or ownership in another business.
Firm Assets	Anything owned, created, obtained, or compiled by or on behalf of the firm, including physical property, technology (hardware, software, and information systems), financial assets (such as cash, bank accounts, and credit standing), and information assets (such as customer lists, financial information, intellectual property, and other data).
Gift	A gift is anything of value for which a person does not pay retail, usual or customary cost. It is broadly defined and includes but is not limited to cash or cash equivalents, business hospitality (including travel and related expenses, meals, entertainment), training and conferences, honoraria and speakers fees, visa letters, an offer of employment or other work experience whether paid or unpaid, products, services, tickets, use of a residence, raffle prize, preferential rates, perks and discounts, charitable or political contributions made on behalf of another, or the use of firm resources. It may include providing anything of value indirectly through a family member, close associate, or business partner.

Relationship Manager	Firm contact/s or employee/s responsible for managing Supplier relationship.
Lobby	Communicate with government officials in an attempt to influence official action.
Material Non-Public Information (MNPI)	Material non-public information, also known as inside information, is information about an issuer of financial instruments (our firm or another) that is not known by the public but if it were, would likely: (1) affect the market price of the financial instruments to which the information relates; (2) influence a reasonable investor to trade those financial instruments; or (3) be used as part of an investment decision regarding those financial instruments.
Personal Information	Information that identifies, is identifiable to, or can be used to identify an individual alone or in combination with other information in the firm's possession.
Political Contribution	Direct or indirect contributions to candidates, campaigns, political parties or committees. This includes in-kind contributions such as the use of firm resources.
Supplier	Any third party, firm or individual that provides a product or service to the firm, including suppliers, vendors, consultants, agents, contractors, temporary workers, third parties working on behalf of the firm as well as the owners, officers, directors, employees, consultants, affiliates, contractors and subcontractors of these organizations and entities.

JPMC DRUG TESTING POLICY

Supplier shall be responsible for determining, by random selection or other lawful and appropriate means, which Designated Supplier Personnel are required to take a drug screening test prior to the first day of their assignment at JPMorgan Chase & Co. (including its subsidiaries and affiliates "JPMC"). Supplier must ensure and warrant that, at all times, a minimum of five (5) percent of all Designated Supplier Personnel who are onboarded at JPMC have passed a drug test within ninety days prior to their start date. "Designated Supplier Personnel" are Supplier personnel as defined in the agreement for services between JPMC and Supplier. In the event that Designated Supplier Personnel are not defined in an agreement, Designated Supplier Personnel means any Supplier personnel that (i) work at a site of any JPMC and receive a JPMC identification access badge, or (ii) have the ability to write, alter, modify, remove or delete (A) JPMC confidential information; (B) the networks or systems of any JPMC; or (C) property of JPMC or its customers (tangible or intangible).

Drug testing will be conducted by Supplier at Supplier's expense. JPMC, at its discretion, has the right to audit Supplier's drug test records and procedures pertaining to Designated Supplier Personnel.

It is Supplier's responsibility to warrant that it will use a drug test laboratory that is Substance Abuse Mental Health Service Administration (SAMHSA) certified and will conform to the minimum JPMorgan Chase & Co. Health Services Drug Testing Standards, a current copy of which is attached hereto as Appendix 1.

During Designated Supplier Personnel's assignment with JPMC, the Supplier Personnel must be able to carry out their jobs in a working environment that is free from alcohol and drug misuse. Designated Supplier Personnel must not, at any time, conduct business while under the influence of prohibited drugs or alcohol. During Designated Supplier Personnel's assignment with JPMorgan Chase & Co., if there is reason to believe that their work is being impaired as a result of alcohol and/or drug misuse, Supplier may be required to have such Designated Supplier Personnel undergo a drug screening test in order to remain on such assignment. Under certain circumstances, Designated Supplier Personnel may also be asked to take a random test for drugs or alcohol if they perform a job that could affect the safety of themselves or others. If Designated Supplier Personnel refuse to cooperate in a drug screening test, they may be subject to immediate removal from their assignment.

Supplier must notify Designated Supplier Personnel that in the event they are convicted of any drug-related crime involving the sale, manufacture, distribution of or trafficking in controlled substances, they must immediately notify Supplier, who in turn must immediately notify JPMC, and such member of Designated Supplier Personnel will no longer be eligible for such assignment. If such Designated Supplier Personnel fails to so notify Supplier, corrective action may include immediate removal from their assignment.

Compliance with the procedures set forth above will not relieve Supplier of its obligation to review its personnel or subcontractor's personnel applications and the JPMC Pre-Assignment Statements, or of its obligation regarding the selection, placement and supervision of

Designated Supplier Personnel.

APPENDIX 1 TO JPMC DRUG TESTING POLICY

JPMORGAN CHASE & CO. HEALTH SERVICES DRUG TESTING STANDARDS

Testing must be performed at a Substance Abuse Mental Health Service Administration (SAMHSA) certified laboratory.

The urine specimen must be collected via the Chain of Custody (COC) Protocol. The urine specimen must be tested for the following:

Substances:

1. Amphetamines
2. Cocaine
3. Opiates
4. Phencyclidine (PCP)

Agents:

1. Creatinine
2. Nitrite
3. PH

If the preliminary screening is a positive result, a confirmation test - Gas Chromatography/Mass Spectroscopy (GC/MS) - must beperformed.

All positive results must be reviewed by a Medical Review Officer (MRO).

If you have any questions, regarding this standard, please contact Rebecca Mazzella as the contact for drug testing questions. Please use phone number 212-270-5558.