Dear Valued Supplier,

Insider threats pose significant risks to organizations, requiring the private sector to remain vigilant against both intentional and unintentional internal actors. A single insider incident can result in substantial financial loss and severe reputational harm, whether caused by malice, negligence, accident, or influence from hostile nation-states and non-state actors.

What is an insider threat? JPMorgan Chase ("JPMC" or "the firm") defines an insider threat as the intentional or unintentional misuse of legitimate access to systems, data, or facilities by workforce members, such as employees or contractors. This misuse can exploit vulnerabilities and lead to negative impacts like data theft, sabotage, or fraud, affecting the organization's assets, reputation, and or operations.

JPMC is committed to protecting the security of our workforce, assets, and stakeholders. We remind our customers and clients that bad actors continually target the financial sector, including supply chain partners, using various tactics to access proprietary information, often through insiders.

As an important supplier to JPMC, we would like to take this opportunity to underscore the commitment to the exercise of best practices by highlighting common types of insider threats and key prevention, detection, and mitigation techniques.

Types of Insider Threats:

- **Intentional** threats occur when a workforce member deliberately acts with malicious intent, often for personal gain, revenge, or external benefit. Common examples include unauthorized data disclosure, credential theft or falsification, harassment or manipulation, collusion with external actors, data exfiltration, supply chain compromise, sabotage, and misappropriation of intellectual property.
- **Unintentional** threats occur when a workforce member exposes the organization to risk through accidental or negligent actions, often by failing to follow security policies. For example, a negligent insider may lose devices, access sensitive systems carelessly, or ignore security updates, while an accidental insider creates risk through mistakes or lack of awareness, such as clicking on phishing emails or sharing sensitive documents with the wrong recipients.

Preventative, Detective and Mitigation Techniques:

- **Safeguarding Critical Assets:** Identify and protect critical assets, ensuring controls are in place that are designed to prevent misuse, unauthorized access, or loss of data.
- **Access Controls:** Ensure that only authorized personnel, operating under the principle of lease privilege, have access to sensitive information, systems, facilities, and physical areas, and conduct regular reviews and updates of permissions to reflect changes in roles and responsibilities.
- **Onboarding/Offboarding Processes:** Implement robust onboarding procedures that provide thorough training on security protocols and policies and establish effective offboarding processes designed to ensure prompt revocation of access to system, data, and facilities.
- **Background Checks:** Perform risk-based pre-employment and pre-engagement screenings to verify candidate backgrounds, including education, employment history, and other relevant factors, to identify and mitigate potential risks.
- **Supply Chain Diligence:** Evaluate vendors and network partners to ensure that third parties are free from sanctions, restrictive regulations, or insider risk behaviors, while also assessing supply chain dependencies to identify and mitigate vulnerabilities that could compromise operational continuity, security, and compliance.
- **Behavioral Detection:** Develop criteria for detecting anomalous work patterns - such as irregular hours, unusual work habits, or attempts at data exfiltration and/or intrusion- by implementing monitoring tools and protocols that enable swift identification and mitigation of potential risks.
- **Workforce Reporting:** Invest in programs designed to detect risks early, employing a "see something, say something" campaign and regular training to empower the workforce to recognize and report concerning behaviors confidentially and without fear of retribution.
- **Education and Awareness:** Provide regular and tailored education to help employees recognize tactics used by insiders as well as external threat actors, such as criminal groups or nation-state entities, ensuring vigilance in business engagements to protect both themselves and the firm.

We greatly value our supplier relationships and are committed to collaboratively addressing shared threats. If you have any questions about this letter or wish to learn more, please contact jpmc.supplier.notifications@jpmchase.com.

Thank you for your continued confidence in JPMorgan Chase.

Henry W Shiembob
Global Chief Security Officer

Jim Connell
Global Supplier Services