STATE OF CALIFORNIA
Department of Financial Protection and Innovation
GOVERNOR **Gavin Newsom** · COMMISSIONER **Clothilde V. Hewlett**

MEMORANDUM

To: All Financial Institutions Licensed By DFPI

Date: March 4, 2022

From: Commissioner Clothilde V. Hewlett

Subject: Obligations Regarding Situation in Ukraine and Russia

---

Due to the rapidly evolving situation in Ukraine and Russia, the Department of Financial Protection and Innovation ("DFPI") issues this Guidance to remind licensees of their obligations under state and federal law.

SANCTIONS

All U.S. persons, including financial institutions licensed by the DFPI ("licensees"), are subject to the regulations issued by the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC").[1] Therefore, licensees must fully comply with U.S. sanctions on Russia.

OFAC has added Russian individuals and entities to the Specially Designated Nationals ("SDN") List. Licensees are prohibited from engaging in any financial transactions with persons on the SDN List. The SDN List can be found on the U.S. Treasury Department's website. In anticipation of frequent additions, licensees are urged to sign up for email updates directly from the U.S. Treasury.

In addition, more limited, yet stringent, sanctions have been placed on several Russian entities with respect to their ability to raise debt and equity and/or with respect to their correspondent and payable-through accounts. Licensees should review the specific restrictions on the OFAC website to ensure compliance.

Licensees are strongly encouraged to take the following actions immediately:

- Ensure that their systems, programs, and processes comply with OFAC regulations.
- Review transaction monitoring and filtering programs to make any modification that is necessary to capture new sanctions.
- Monitor all transactions going through their institution, particularly trade finance transactions and funds transfers, to identify and block transactions

[1] 31 C.F.R. Chapter V; *see* Cal. Fin. Code, § 580.

subject to sanctions, and follow OFAC's direction regarding any blocked funds.

VIRTUAL CURRENCY

The Russian invasion significantly increases the risk that listed individuals and entities may use virtual currency transfers to evade sanctions. All licensees engaging in financial services using virtual currencies should have policies, procedures, and processes to protect against the unique risks that virtual currencies present. Refer to the OFAC Guidance, OFAC Sanctions Compliance Guidance for the Virtual Currency Industry. Licensees should consider virtual currency-specific control measures including sanctions lists, geographic screening, and any other measures appropriate to the licensee's specific risk profile.

CYBERSECURITY

The Russian invasion significantly elevates the cyber risk for the U.S. financial sector. In order to operate in a safe and sound manner as required by California law,[2] licensees must mitigate cybersecurity threats.[3] Licensees should:

- Adopt core cybersecurity hygiene measures like multi-factor authentication, privileged access management, vulnerability management, and disabling or securing remote desktop protocol access.
- Review and confirm border security configurations to eliminate any networking protocols that are non-essential.
- Ensure that procedures address destructive cyber-attacks such as ransomware and immediately confirm backups are protected from a ransomware attack.
- Re-evaluate plans to maintain essential services, protect critical data, and preserve customer confidence considering the realistic threat of extended outages.

Licensees should closely track guidance and alerts from the Cybersecurity and Infrastructure Security Agency on its 'Shields-Up' website.

Licensees that do business in Ukraine and/or Russia should take increased measures to monitor, inspect, and isolate traffic from Ukrainian or Russian offices and service providers. Licensees should segregate networks for Ukrainian or Russian offices from the global network.

[2] Cal. Fin. Code, § 580.
[3] This Guidance does not supersede any reporting requirements in the event of a cybersecurity incident.