STATE OF CONNECTICUT
DEPARTMENT OF BANKING
260 CONSTITUTION PLAZA – HARTFORD, CT 06103-1800

Jorge L. Perez
Commissioner

TO: **Entities Regulated by the CT Department of Banking ("regulated entities")**

FROM: **Jorge L. Perez, Banking Commissioner**

DATE: **March 10, 2022**

RE: **Situation in Ukraine and Russia and Impact to Financial Services Sector**

The Connecticut Department of Banking ("Department") is closely monitoring the rapidly evolving situation in Ukraine and Russia.

The Department is issuing this Guidance to reiterate that regulated entities should fully comply with U.S. sanctions on Russia, as well as any Connecticut State and Federal laws and regulations. This Guidance provides a non-exhaustive summary of steps that regulated entities should be taking. The Department understands that not every measure applies to every regulated entity. However, in the interest of transparency, the Department is sharing this vital information with all regulated entities.

The Department will provide further guidance to regulated entities as necessary.

SANCTIONS

The President of the United States and other leaders around the globe have imposed severe economic sanctions on Russian individuals, banks, and other entities. The following have been issued by the U.S. Treasury Department:

- U.S. Treasury Announces Unprecedented & Expansive Sanctions Against Russia, Imposing Swift and Severe Economic Costs
- U.S. Treasury Targets Belarusian Support for Russian Invasion of Ukraine
- Ukraine-/Russia-related Sanctions

The U.S. Treasury Department's Office of Foreign Assets Control ("OFAC") has added individuals and entities to the Specially Designated Nationals ("SDN") List. The SDN List can be found on the U.S. Treasury Department's website. In anticipation of frequent additions, regulated entities are urged to sign up for email updates directly from the U.S. Treasury to ensure timely implementation of any further sanctions.

U.S. persons (including, without limitation, banks, credit unions, virtual currency businesses, and other financial institutions) are prohibited from engaging in any financial transactions with persons on the SDN List, unless OFAC has authorized otherwise.

While not on the SDN List, 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. Regulated entities must review the specific restrictions as contained on the OFAC website to ensure continued compliance.

Regulated entities should take the following actions immediately:

- Monitor all communications from the Department, the U.S. Department of the Treasury, OFAC, and other Federal agencies on a real-time basis to stay abreast of the latest developments to ensure that their systems, programs, and processes remain in compliance with all the requirements and restrictions imposed.
- Review Transaction Monitoring and Filtering Programs to make any modification that is necessary to your systems to capture the new sanctions as they are proposed, and to ensure continued compliance with all applicable laws and regulations.
- Monitor all transactions going through your institution, particularly trade finance transactions and funds transfers, to identify and block transactions subject to the OFAC sanctions, and follow OFAC's direction regarding any blocked funds.
- Ensure that OFAC compliance policies and procedures are being updated on a continuous basis to incorporate these sanctions and any new sanctions that may be imposed on additional entities.

VIRTUAL CURRENCY

The Russian invasion also significantly increases the risk that listed individuals and entities may use virtual currency transfers to evade sanctions. Accordingly, all regulated entities engaging in financial services using virtual currencies must have tailored policies, procedures, and processes to protect against the unique risks that virtual currencies present. Refer to the OFAC Guidance, Sanctions Compliance Guidance for the Virtual Currency Industry.

Regulated entities should pay special attention to the effectiveness of virtual currency-specific control measures including, but not limited to, sanctions lists, geographic screening, and any other measures relevant to each entity's specific risk profile.

Examples of some virtual-currency-specific internal controls include:

- Use of geolocation tools and IP address identification and blocking capabilities to detect and prevent potential sanctions exposure.
- Transaction monitoring and investigative tools, including blockchain analytics tools, to identify transaction activity involving virtual currency addresses or other identifying information associated with sanctioned individuals and entities listed on the SDN List, or located in sanctioned jurisdictions.

Regulated entities should have policies, procedures, and processes in place to implement necessary internal controls, with appropriate training, risk assessments, and testing and auditing against their risk profile.

CYBERSECURITY

The Russian invasion of Ukraine significantly elevates the cyber risk for the U.S. financial sector. Escalating tensions between the U.S. and Russia also increases the risk that Russian threat actors will directly attack U.S. critical infrastructure in retaliation for sanctions or other steps taken by the U.S. government.

To mitigate cybersecurity threats, regulated entities should:

- Review programs to ensure full compliance, with particular attention to core cybersecurity hygiene measures like multi-factor authentication ("MFA"), privileged access management, vulnerability management, and disabling or securing remote desktop protocol ("RDP") access.
- Review and confirm border security configurations to eliminate any networking protocols that are non-essential.
- Review, update, and test incident response and business continuity planning, and ensure that those plans address destructive cyber-attacks such as ransomware.
- Immediately confirm backups are protected from a ransomware attack and have and maintainan updated incident response plan.
- Re-evaluate plans to maintain essential services, protect critical data, and preserve customer confidence considering the realistic threat of extended outages and disruption.
- Conduct a full test of the ability to restore from backups. Do not assume that backup restoration will succeed until a full test has been successfully completed.
- Provide additional cybersecurity awareness, training, and reminders for all employees.
- Senior management, boards of directors, and other governing bodies of regulated entities should exercise oversight of all such planning and implementation.

Regulated entities should also closely track guidance and alerts from the Cybersecurity and Infrastructure Security Agency ("CISA"), which provides information on its "Shields-Up" website to promote awareness of current cybersecurity threats and mitigations. Regulated entities should review and implement practices not already in place that are recommended in the following CISA issuances:

- Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure.
- CISA Insights Article: Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats.
- CISA Insights Article: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure.

Furthermore, regulated entities 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, including traffic over virtual private networks ("VPNs").

Regulated entities should review firewall rules, active directory and other access controls, and should segregate networks for Ukrainian or Russian offices from the global network.

For cybersecurity incidents, certain regulated entities are subject to additional reporting requirements. This Guidance does not supersede such reporting requirements to your regulator.

In this heightened threat environment, CISA asks that organizations lower their thresholds for reporting incidents to the FBI or CISA to help the U.S. government identify issues and help protect against attacks. Reporting can be made to CISA at https://us-cert.cisa.gov/forms/report, email at central@cisa.gov or (888) 282-0870; and/or to an FBI local field office, or to the FBI's 24/7 CyWatch email at CyWatch@fbi.gov or (855) 292-3937.

If you have any questions, please email your primary point-of-contact at the Department.