NEW YORK STATE OF OPPORTUNITY. | Department of Financial Services

KATHY HOCHUL
Governor

ADRIENNE A. HARRIS
Superintendent

February 25, 2022

To: All Individuals and Entities Regulated by the New York State Department of Financial Services ("regulated entities")

Re: Escalating Situation in Ukraine and Impact to Financial Sector

The New York State Department of Financial Services ("Department" or "DFS") is closely monitoring the rapidly evolving situation in Ukraine given the Russian invasion.

Due to the recent developments, the Department is issuing this Guidance to reiterate that regulated entities should fully comply with U.S. sanctions on Russia, as well as New York State and Federal laws and regulations, including Department cybersecurity and virtual currency regulations set forth in 23 NYCRR 500 and 23 NYCRR 200, respectively. 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.

CYBERSECURITY

The Russian invasion of Ukraine significantly elevates the cyber risk for the U.S. financial sector. Russia's ongoing cyber-attacks against Ukraine could spillover and damage networks outside of Ukraine – as has happened in the past. Escalating tension 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.

The Department expects that this risk is mitigated by the comprehensive risk-based cybersecurity program adopted by each regulated entity pursuant to the Department's cybersecurity regulation (23 NYCRR 500) and subsequent guidance. Regulated entities should:

- Review their 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, update, and test their incident response and business continuity planning, and ensure that those plans address destructive cyber-attacks such as ransomware.
- Review and implement practices not already in place in the Department's June 2021 Ransomware Guidance, which sets forth key controls that reduce the risk of destructive cyber-attacks. Regulated

entities should immediately confirm they have backups that will be protected from a ransomware attack and an updated incident response plan.
- Re-evaluate their 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 their ability to restore from backups. Regulated entities should not assume that they can restore 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") and Information Sharing and Analysis Centers ("ISACs"). Indicators of compromise ("IOCs") for known threat actors should be immediately incorporated into network defenses. And 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.
- 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 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.

Regulated entities must report cybersecurity events that meet the criteria of 23 NYCRR Section 500.17(a) as promptly as possible and within 72 hours via the secure Department Portal, which can be accessed from the Cybersecurity Resource Center. Regulated entities should also report cybersecurity events immediately to law enforcement, including the FBI and CISA at https://www.cisa.gov/uscert.

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 U.S. Treasury Department's Office of Foreign Assets Control ("OFAC") has been issuing orders and guidance on implementation of these sanctions.

All orders and guidance on sanctions, including financial entities on the Specially Designated Nationals ("SDN") List, are accessible on the U.S. Treasury Department's website. In anticipation of frequent additions, regulated entities are urged to sign up on that site for email updates directly from the U.S. Treasury to ensure timely implementation of any further sanctions.

U.S. persons (including, without limitation, banks, virtual currency businesses, insurers and other financial institutions as well as insurance producers and third-party administrators) are prohibited from engaging in any financial transactions with persons on the SDN List, unless OFAC has authorized otherwise, through licenses listed on the OFAC website, or by obtaining a separate license for a particular transaction. 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 their Transaction Monitoring and Filtering Programs to make any modification that is necessary to their systems to capture the new sanctions as they are proposed, and to ensure continued compliance with all applicable laws and regulations, including Part 504 of the Superintendent's Regulations.
- Monitor all transactions going through their institutions, 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 their 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 virtual currency transfers may be used to evade sanctions for listed individuals and entities, including through transmission of virtual currency to or from users located in comprehensively sanctioned jurisdictions. Accordingly, all regulated entities engaging in virtual currency business activity — including but not limited to a BitLicensee or a Limited Purpose Trust Company — must have tailored policies, procedures, and processes to protect against the unique risks that virtual currency present including through implementation of existing federal and Department guidance related to sanctions compliance. These include but are not limited to:

- OFAC Sanctions Compliance Guidance for the Virtual Currency Industry.
- Part 200 Virtual Currencies and, specifically, Section 200.15 Anti-Money Laundering Program.

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 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.

If you have any questions, please email your primary point-of-contact at the Department and copy info@dfs.ny.gov, which is continuously monitored as this situation unfolds.

Sincerely,

Adrienne A. Harris, Superintendent

New York State Department of Financial Services