State of New Jersey
DEPARTMENT OF BANKING AND INSURANCE
OFFICE OF THE COMMISSIONER
PO BOX 325
TRENTON, NJ 08625-0325
TEL (609) 633-7667

PHIL MURPHY
Governor

SHEILA OLIVER
Lt. Governor

MARLENE CARIDE
Commissioner

BULLETIN NO. 22-05

TO: **ALL INDIVIDUALS AND ENTITIES REGULATED BY THE DEPARTMENT OF BANKING AND INSURANCE**

FROM: **MARLENE CARIDE, COMMISSIONER**

RE: **ESCALATING SITUATION IN UKRAINE AND ITS IMPACT ON DEPARTMENT REGULATED ENTITIES**

On March 2, 2022, Governor Phil Murphy issued Exec. Order No. 291 (March 2, 2022) ___ N.J.R. ___ ("EO 291"). EO 291 directed the Department of Banking and Insurance ("Department") to issue bulletins or directives to its appropriate regulated entities, requiring them to fully comply with United States sanctions on the Russian Federation and Belarus, as well as with New Jersey laws and regulations and federal laws and regulations.

Pursuant to EO 291, the Department is issuing this Bulletin to reiterate that regulated entities should fully comply with U.S. sanctions, including those on Russia and Belarus, as well as with New Jersey laws and regulations and Federal laws and regulations. This Bulletin provides a non-exhaustive summary of steps that regulated entities should be undertake at a minimum. The Department understands that not every measure applies to every regulated entity; however, in order to be thorough, the Department is sharing this vital information with all regulated entities.

Cybersecurity

Regulated entities should evaluate their systems for cyber risk and take appropriate actions to mitigate cyber risk. The Russian invasion of Ukraine significantly elevates the cyber risk to the U.S. financial sector. Russia's ongoing cyber-attacks against Ukraine have the potential to damage

networks beyond Ukraine. Borders do not exist in cyberspace, and once malware is deployed, it has the potential to infect systems across the globe. Further, Russian actors may directly attack U.S. critical infrastructure in retaliation for sanctions or other steps taken by the U.S. government. Along with cyber threat activity, Russia is likely to engage in disinformation campaigns in attempts to garner support for the Russian Government and their actions, and/or to sow unrest and division. To help guard against cyber-attacks, regulated entities should:

- Review their programs to ensure full compliance, with particular attention to core cybersecurity 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.
- Re-evaluate their plans to maintain essential services, protect critical data and preserve customer confidence in consideration of the realistic threat of extended outages and disruption.
- Conduct a full test of their ability to restore their systems and data from backups. Regulated entities should not assume that they can restore such systems and data until a full test has been successfully completed.
- Provide additional cybersecurity awareness training and reminders for all employees.

Best industry practices for cybersecurity can also be found at https://www.nist.gov/cyberframework. The Conference of State Bank Supervisors ("CSBS") also has information of cybersecurity at https://www.csbs.org/cyber101-legacy. 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 incorporated immediately into network defenses. 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.

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 virtual private networks ("VPNs"). Regulated entities also should review firewall rules, all active access controls, and should segregate networks for Ukrainian or Russian offices from the global network.

Regulated entities should also report cybersecurity events immediately to law enforcement, including the FBI and CISA at https://www.cisa.gov/uscert. In New Jersey, you should also file a report with the New Jersey Cybersecurity & Communications Integration Cell ("NJCCIC") at www.cyber.nj.gov. NJCCIC also offers a free membership to receive alerts, advisories, bulletins, and training notifications.

Sanctions

Global leaders have imposed severe economic sanctions on Russian individuals, banks, and other entities. The United States Department of Treasury's Office of Foreign Assets Control ("OFAC") has been issuing orders and guidance on implementation of these sanctions.

The Department expects all regulated companies to comply with the requirements of OFAC, which has recently released guidance relating to Russian and Belarusian individuals, companies, and other entities. All orders and guidance on sanctions, including financial entities on the Specially Designated Nationals ("SDN") List, are accessible on the United States 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 banks and credit unions, 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 regarding to their ability to raise debt and equity with respect to their correspondent and payable-through accounts. Regulated entities should 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 Treasury, OFAC, and other Federal agencies on a real-time basis to stay updated on 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.

- 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.

Banking

The Department charters and maintains broad statutory authority over the banks, savings banks, savings associations and credit unions, together with the consumer finance licensees, specifically money transmitters and foreign money transmitters (collectively "Money

Transmitters"). These regulated entities and licensees are closely monitored by the Department through its oversight and examination processes. The Department ensures that material financial conditions and operations are safe and sound and not subject to excessive risk. The Department reminds regulated entities and licensees that they 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, and that they should report any suspicious activities timely with FinCEN and applicable law enforcement agencies.

As part of the application for licensure with the Department, Money Transmitters must identify each country that they would transmit to or receive from. See N.J.S.A. 17:15C-7(a)10. In the annual reports, Money Transmitters are required to notify the Department of material changes to information provided in the application. See N.J.S.A. 17:15C-12(d)3. The Department considers the countries the Money Transmitters send or receive to or from to be material information.

Of particular importance at this time, Money Transmitters should ensure that their transaction oversight appropriately identifies designated individuals, entities and countries sanctioned by OFAC. Money Transmitters who currently send to and receive from correspondent banks or payable through accounts located in Russia or Belarus shall submit a report that includes an assessment of the impact of the current sanctions and an implementation plan to address the same ("Money Transmitter Report for Bulletin No. 22-05"). The Money Transmitter Report for Bulletin No. 22-05 should be submitted within thirty (30) days of this Bulletin to bliconline@dobi.nj.gov.

Insurance

The Russian invasion of Ukraine significantly elevates the risk throughout the insurance sector. Russia's ongoing attacks against Ukraine could affect risks, including but not limited to,

market, credit and liquidity risk, cyber and operational risk, strategic and other risks. The Department expects risks will be mitigated by a comprehensive risk management process overseen by senior management and Boards of Directors of insurance entities authorized to do business in New Jersey.

The Department maintains broad statutory authority over insurers relating to corporate governance, risk management, investment management, and internal controls. In addition, enterprise risk filings (Form F) pursuant to N.J.S.A. 17:27A-3(k) are expected to include reporting on these risks for any company which is a member of an insurance holding company system and where New Jersey is the lead state regulator. Regulated entities are reminded of their obligation to actively identify and manage risks and actively engage with the Department, as needed. The report shall, to the best of the ultimate controlling person's knowledge and belief, identify the material risks within the insurance holding company system that could pose enterprise risk to the insurer. The Department reminds regulated entities to 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.

Compliance

The Department may take administrative action, including suspending or revoking licenses, permits, registrations, and certifications of regulated entities owned or controlled by the government of Russia, Belarus, or their instrumentalities, and businesses that invest directly in such companies. The Department may revoke, suspend, refuse to issue licenses, or take other administrative action under the following non-exhaustive list of authorities:

- N.J.S.A. 17:1-15 (general powers and duties of Commissioner)
- N.J.S.A. 17:1-28 (causes for revocation, suspension, refusal to issue or renew a bank, savings bank, State association license)
- N.J.S.A. 17:15C-16 (suspension, revocation of license of Money Transmitters)

- N.J.S.A. 17:15C-23 (permits injunctions for violating or about to violate Money Transmitters Act)
- N.J.S.A. 17:22A-40 (causes for revocation, suspension, or refusal to issue or renew insurance producer license)
- N.J.S.A. 17:11C-7 (conditions for issuance of license to lenders)
- N.J.S.A. 17:11C-18 (Commissioner's authority to revocation of licenses)
- N.J.S.A. 17:11C-70 (authority of Commissioner for issuing licenses to lenders)
- N.J.S.A. 17:16F-30 (requirements for licensure as a mortgage servicer)
- N.J.S.A. 17:51A-1 to -5 (Administrative Supervision of insurers)
- N.J.A.C. 11:2-27.3 to -.4 (factors to determine whether an insurer is in an hazardous financial condition, including engaging in unlawful transactions, and gives Commissioner authority to take actions as she deems necessary to protect the insurer's policyholders, creditors, or the general public).
- N.J.S.A. 45:15-9 (requires good moral character of applicants for a real estate license)
- N.J.S.A. 45:15-12.4 (revocation of real estate partnership or corporate license)
- N.J.S.A. 45:15-17 (causes for suspension or revocation of real estate licenses)
- N.J.S.A. 45:15-16.42 (Real Estate Commission empowered to issue Cease and Desist Orders)
- N.J.S.A. 45:15-16.43 (Revocation of registration of land subdivider)

The Department will continue to closely monitor the situation in Ukraine given the Russian invasion and provide further guidance to regulated entities as necessary.

3/17/2022

Date

Marlene Caride
Commissioner

jd rus sanctions bul/bulletins