Hello, and good morning to all of you. My name is Elizabeth Rosenberg, and I am the Assistant Secretary for Terrorist Financing and Financial Crimes at the U.S. Department of the Treasury. It is my pleasure to address this group again. Much has changed in the world since I spoke to you back in February. Most notable for this group, of course, is Russia’s invasion of Ukraine and the economic consequences that followed.

Russia’s illegitimate and brutal invasion of Ukraine united over 30 countries of the world, representing more than half of the world’s economy, to impose the largest sanctions regime in modern history. And as long as Russia’s invasion of Ukraine persists, so too will our global and coordinated efforts to impose costs on Russia and limit its ability to pursue this war of aggression.

Our most recent sanctions designations exemplify this effort—the United States Treasury took action against Russia’s military-industrial supply chain, as well as some of its top financial leadership who are seeking to exploit the international financial system to fund Putin’s war. And Russia is working to exploit the global financial system—not just to raise and move money to fund an illegal and unjust war, but to evade the sanctions and financial controls in dozens of countries that are designed to protect financial integrity, stability, and growth.

Your financial institutions, much like ours, are vulnerable to the Russian aiders and abettors of this war. There are public reports that Russian money laundering is active in the Arab world. This is something we all have a vested interest in preventing, investigating, and eliminating.

Russia’s invasion has certainly upended many things; this includes disrupting global supply
chains and spiking grain and energy costs. But one thing has remained constant, and has even been clarified, through our renewed focus in following Russia’s money: the vulnerabilities Russia exploits in the international financial system are neither novel nor unique.

The corrupt cronies in Putin’s inner circle are using the same loopholes that others use to hide their ill-gotten gains: shell companies, proxies, corrupt gatekeepers, and weak anti-money laundering frameworks. Further, they seek to protect and reinvest their assets by moving them abroad and storing them in valuable sectors like real estate.

Unfortunately, these practices originate in your countries as well. Take Lebanon, for example. Since October 2019, Lebanese elites have ignored the public’s calls for transparency and reform, while shielding their own assets from depreciating, by transferring their own money out of the country to other jurisdictions. The U.S. Treasury estimates that since the beginning of the October 2019 protests, Lebanese banks allowed some customers to transfer at least $456 million to their own foreign accounts. Of course, it is not illegal or illicit to move money out of Lebanon. But can the international financial community discern that all these funds were properly screened and vetted at the appropriate level for politicians and businessmen potentially engaged in corruption? Or were some elements of the international financial community complicit in moving the proceeds of corruption? Or depriving the Lebanese people of funds that should be available to them in Lebanon? Where are these funds now?

These are challenging questions. The United States grapples with them in many respects as well—U.S. financial sector leaders and compliance professionals have a responsibility and obligations to rigorously undertake the various tasks of protecting the financial system’s integrity and stability. Notwithstanding all our efforts, the United States remains a preferred destination for many illicit financiers. That is why we are taking concrete action.

On September 29, the U.S. Treasury’s Financial Crimes Enforcement Network, also known as FinCEN, issued a new rule on beneficial ownership information reporting requirements. This represents a historic shift in financial transparency for the United States. The rule will require certain entities to disclose information about their beneficial owners and the individuals who formed them—that is, the real people who actually own, control, or created these companies. This requirement will apply to certain foreign entities registered to do business in the United States as well.

We are also working with each of your governments to increase financial transparency and
accountability requirements to align with international standards. However, governments generally do not move or innovate as quickly as the private sector, and there are steps you all can take right now to shore up some key vulnerabilities. This is particularly relevant for jurisdictions such as Iraq, for instance, where some politicians, driven by corruption and foreign interference, are actively undermining transparency and reform efforts.

I’d like to take the opportunity today to call out two key vulnerabilities revealed by our heightened attention to Russian money laundering: (1) a transformed risk associated with corrupt elites, and (2) the lack of transparency into the real estate sector.

When I spoke here previously I touched on the evolving risks posed by corrupt elites —and some of those warnings are now being realized, unfortunately. Designated Russians have turned to family members, associates, and anonymous shell companies in jurisdictions with weaker controls to obfuscate their ill-gotten gains and maintain connectivity to the international financial system. And even as the United States and our partners designate many individuals publicly, there are other illicit actors in their corrupt patronage networks laundering money on their behalf.

For financial institutions like yours, it is not enough to check the U.S. Treasury Office of Foreign Assets Control’s sanctions listings in order to vet high-risk customers. The UK and EU are also taking unprecedented action against corrupt individuals. While these lists are coordinated, they are not identical. I strongly encourage you all to pay close attention to UK and EU sanctions actions, and to use them to form the appropriate enhanced due diligence procedures for high risk persons in your financial systems. In the coming months, my teams will be traveling to jurisdictions known to have unusual financial flows tied to Russian oligarchs and elites to share information and, as appropriate, to encourage investigations.

For real estate, there has been public reporting about an increase in Russian purchases abroad, and particularly in the Gulf. Some of these purchases and investments could be used to evade multilateral sanctions. Your increased vigilance will be essential to be sure that your jurisdictions are not participating in the laundering of the proceeds of corruption or facilitating sanctions evasion, among other crimes. For example, this summer the UAE Ministry of Economy announced new regulations and reporting requirements for cash purchases of real estate, as well as reporting requirements for any purchase made with virtual assets or from proceeds of virtual asset sales.

This information and other enhanced regulatory measures will be critical to identify and
disrupt any Russian illicit finance or sanctions evasion activity. I encourage you all to familiarize yourselves with the Risk-Based Approach Guidance for the Real Estate Sector published by the Financial Action Task Force in July of this year. I also encourage you to elevate your scrutiny of transactions related to the real estate sector, and to communicate with all your partners—whether they be real estate agents, lawyers, notaries, developers, insurances, and accountants—to ensure they are not funnelling the proceeds of corruption or unwittingly abetting international money laundering.[1]

When I spoke to you last, I charged you all to remain vigilant against corruption, share information with one another, and invest in robust compliance programs. I know the Union of Arab Banks has held AML/CFT workshops since that time, which I was pleased to see. Yet the hard work continues. Every financial institution represented here today provides essential services to individuals, business, and entities—and the services must continue. Alongside these essential services, we all have a responsibility to keep illicit and corrupt activity out of our systems. I look forward to continuing our work on this, together.

Thank you.

###