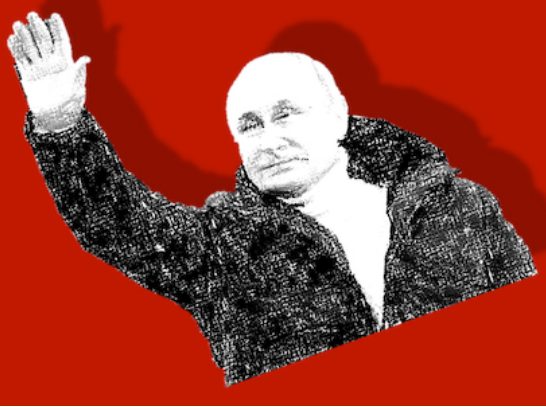

March 23, 2022

Tanks and Banks:

What Fintechs Must Know About Economic Sanctions on Russia

Edited by Tom Hagy, Featuring Brad Rustin of Nelson Mullins Riley & Scarborough

This is an edited version of my interview with **Brad Rustin of Nelson Mullins Riley & Scarborough**, a highly regarded attorney and much-sought-after speaker for his expertise on the laws and operations of the technology-driven global financial system. It is based on Rustin's appearance on the **Emerging Litigation Podcast**, produced by HB Litigation and Law Street Media. In the spirit of the movie "This Is Spinal Tap," if sanctions came with a volume knob, those leveled at Russia would be turned to 11. Russian banks and businesses, oligarchs, government officials are all feeling the squeeze of banned transactions, frozen accounts, and confiscated property. The Russian national wealth fund is now as frozen as a Siberian mammoth. Russian banks no longer have access to the SWIFT international payment system. The country is teetering on the brink of its first default on international debt since the Bolshevik Revolution a century ago. While some argue that sanctions are nothing compared to military action, they are impeding Russia's ability to fund its activities at home and abroad. Putin himself refers to them as an "economic blitzkrieg," no doubt keeping with his "anti-Nazification" theme. The Wall Street Journal reports that, in addition to potentially defaulting on its debt, the sanctions are causing "factory closures, job losses, a doubling of interest rates and a decline of the ruble," and "inflation has galloped ahead of the central bank's target." U.S. and European Union sanctions have "hammered the Russian economy, cutting off much of Russia's financial system from the rest of the world and choking off the flow of many imported goods," WSJ reports. Global fintechs and companies should read on for insights into staying on the right side of these sanctions. –**Tom Hagy**, Host, Emerging Litigation Podcast, Founder, HB Litigation, Contact: Editor@LitigationConferences.com

What are the different types of sanctions programs?

Compared to the last 40 or 50 years, these are the most robust set of sanctions that the U.S. government has ever attempted to impose. Its impact is obviously being magnified by our allies in the European Union, in the G7, and the G10. When we think about these different sanctions, they are targeting the Russian Federation's entire access to the financial system, which is almost unprecedented. They are going after industries, banks, and individuals. That's unique. Traditionally, when we institute sanctions programs the Office of Foreign Asset Control or OFAC, a division of the U.S. Treasury Department, puts you on a list of Specially Designated Nationals (SDMs). These are people you cannot do business with and, in some limited circumstances, there are countries you can't deal with, such as Iran and North Korea. This is the first time we've seen broad sector sanctions in banking and finance, real estate, and energy. We have political persons being put on the SDN list, too.

This is one of the most robust sanctions programs we've ever seen.

Tell us more about OFAC and its impact on fintechs.

OFAC applies not only to banks and fintechs, but generally to anyone conducting commerce in the U.S. It's one of the few Treasury agencies that really crosses over, in, and out of the financial services space. In terms of how it's impacting the banks and fintechs, you have to think about their compliance programs. Treasury reporting entities -- banks, credit unions, money services, anyone who moves and transmits money -- all have to perform anti-money-laundering functions. On top of that, they're performing sanction screening. Anyone who is a Treasury-regulated entity received this list of sanctions. In the space of a few days, they had to institute blocking programs, rejection programs, and screening programs, the latter being the most important. They will have to go through their customer lists to make sure none of them are impacted by the sanctions. There wasn't a lot of time to do it. A lot of the banks and fintechs are scrambling to catch up. This only works if a bank or fintech had a robust "know your customer" policy. This means that when you signed up to work with that fintech or bank, they did a good job identifying who you were.

If that onboarding process is broken, then there's really nothing you can do to implement the sanctions programs. That's what is most scary for some of the fintechs, that is, those who are relying on processes they set up five, six or seven years ago.

What types of transactions are being blocked? People are trying to access money around the world, make payments, transfer funds. What transactions are we talking about?

It runs the spectrum. There are not only prohibitions on the transfer of funds, but also on certain debt that's being issued to individuals in the Russian Federation. For example, you can't make

loans with terms longer than 30 days. On top of that, we see for the first time “fintech wars,” where Visa and MasterCard have turned off access to credit cards in the Russian Federation. That applies to everybody. We've seen collaboration between the European Union and the U.S. to turn off SWIFT, the wire payment system that settles with banks, all over the world. If you're making an international payment, there's a 75-plus percent chance it was running over a SWIFT rail. That’s being blocked now for a number of banks. It truly is the first time when the G10 nations, the 10 most economically developed nations in the world who also control SWIFT, have started a comprehensive program to just cut a nation off from fintech and financial services. If you need to make payments inside of Russia now, you have to use Russian domestic wire transfers. Some think the Chinese infrastructure is going to be redeployed to help Russia. But the world turned off the access for the Russian Federation and that really is unprecedented.

Some think the severity of these sanctions is even more aggressive than sending troops.

Instead of deploying military forces, we saw the collapse of the 11th largest economy in the world in the span of two weeks.

I read that some Ukrainians suddenly don't have access to their funds. Have you seen that?

Absolutely. Both in Ukraine and Russia there are liquidity problems. If you can't get other people's currency coming into your country, it's very hard to withdraw your money or get access. Banks all over the world keep about 5-to-7% of the money that they have on deposit that is actually liquid. It's called fractional banking. There is no way for you to make a full withdrawal of all the money that sits in any of these banks.

What about cyberwar?

We’re seeing a spike in hacking and denial of service attacks. The Ukrainian development community, which is one of the most advanced, particularly their financial services technology development teams, are attacking the Russian Federation and the Russian Federation is launching attacks against Ukrainian banks and financial services. [Thousands of volunteer hackers from around the world are teaming up to target Russia, too.]

People around the world have been supporting Ukraine by booking Airbnbs in the country as a way of getting money directly to Ukrainians. Would you say this is risky? [As of this writing, more than $40 million was sent this way.]

Airbnb has made a huge push both to help house refugees as well as making bookings for their Ukrainian hosts. The real challenge will be -- and this has nothing to do with Airbnb as I think their intentions are very good -- is the ability of those hosts to withdraw funds. I feel very confident Airbnb is going to send the money to the account they have on file for those Ukrainian nationals. It's a question of whether hosts can access those funds.

What about cryptocurrency? What role will it play?

There's been a big push to use alternative asset classes. One of the big concerns that a lot of us who work in this industry have is, what is the promise of digital assets? Can cryptocurrencies be used to help get funds to Ukraine? That's what a lot of the big coin exchanges are touting. Is this also a way for Russia to bypass sanctions programs? It's a little bit of both. We've seen a huge uptick in the number of individuals in the Russian Federation trying to use crypto to either liquidate overseas non-ruble-denominated accounts into crypto. At least initially there was a big push of folks trying to load funds into crypto. Obviously, the way the U.S. has regulated so far is we block you from taking the money out. But that doesn't mean you can't put it in an exchange in Malta, Hong Kong, or Singapore, and potentially access it. So, there are ways to bypass sanctions. But the U.S. is blocking the unloading of money and exchanging crypto assets for U.S. dollars inside of the U.S. The other point the exchanges make is it's also a really good way to move value to these individuals in the Ukraine where they have access to something that has value even if their bank may not be open and operating, processing, and functioning. Because if you think about it, the infrastructure to process card transactions for Ukrainian bank takes dozens of people. And the processors have hundreds and thousands of people who are now not able to sit in a center and process your credit card payments. It's really a challenging time to get access to those funds.

You use the terms "rejecting" and "blocking" transactions. What's the difference?

A lot of people don't realize that if you try to send money to a specially designated national, it's not just the institution will say "we can't take the transaction," but "we're going to accept the transaction, call up the U.S. Treasury, put it in a separate account and freeze the funds until the U.S. government, maybe three, four, five or 10 years later, decides what they're going to do with that money." For instance, if you went into a bank and said, "I need to pay somebody in Crimea for some software," the bank will say, "I'm sorry, we can't take that transaction." It's different if you say, "I want to send money to Vladimir Putin." Then the bank is going to take your money, put it in a separate account, and call the good folks at Treasury who will block it and keep the money. It's something businesses need to be aware of. If someone is on an SDN list, their bank is not going to necessarily tell them it's been rejected.

Instead, they're going to take the money, freeze it, and, in essence, embargo it. Other parties still don't get paid and you don't get the money back.

Do these sanctions apply just to people?

That's another unique aspect of this program is it goes much beyond just individual people. If you intend to pay certain companies, you need to check them against the sanctions lists. For instance, a lot of the Gazprom entities (Russia's mostly state-owned energy company) in the energy space, or certain military equipment entities, have all been placed on the list. So, it's not just the people. You cannot just screen who the *person* is who's receiving the funds. If you're going to send money to a business in the Russian Federation, make sure they're not on one of the

entity lists to make sure that that transaction is going to process where it's appropriate. That's assuming you still want to send the money. We've seen fintechs and banks cut ties with the Russian Federation.

How should U.S. fintechs think about doing business in Eastern Europe and Russia?

First, you obviously need to think about what your corporate policy is from a social policy standpoint. That's the calculus that each company's going to make. Do you want to do business with Russia?

Second is, realistically, can you pay the people? Assuming you did want to do business with someone in Russia, is that company or are those people blocked? Will you really be able to pay them? That may be a challenge.

Third – and this is what is scaring the fintech and bank communities the most – is both countries are engaging in cyber war. They are trying to exploit vulnerabilities and disclose confidential data. There are huge development centers in Ukraine and they're all the subject of attacks by hackers in Russia, or allegedly from Russia and other nations supporting Russia. Ukraine has hacking teams that are doing the same thing to Russia. If you're a fintech and you're sending your customer data to Ukraine or to Russia for processing, or you're sending them your scripts and your code, you need to be aware there is a pretty significant cyber risk. Companies need to consider these vulnerabilities when reviewing engagements with those countries.

What are some specific risks to fintechs, banks, and businesses?

The risk flows in a number of different ways. First, obviously, is that you risk sponsoring block transactions. That's the most critical and the most pressing. You must ask: Is your fintech properly ingesting these OFAC sanctions, processing them, and then running the sanctions lists against your customer list? Are you doing a good job knowing who your customer is? You must have a good faith basis to believe you've confirmed their identity. Second, you need to look at your vendor lists and make sure you're not exposed to a vulnerability either in Ukraine or the Russian Federation. Third, you have payment risk. If you're doing business with individuals in the Russian Federation, they may not be able to pay you.

If you're transacting business where you're paying vendors in the Russian Federation, you may not have an effective way to pay them for the next few years. It all depends on how the sanctions programs play out.

What kinds of actions does OFAC take if you violate these sanctions?

They are fairly significant. OFAC can go all the way up to issuing severe fines and penalties, including against individuals. If you look at settlements in the past, generally a fintech or bank is going to have to repay the U.S. Treasury for any transactions that should have been blocked. And

they'll make you go back and do scrubs of those transactions. You're on the hook. It doesn't matter who benefited from the transaction or if it somehow got back to the U.S. or it didn't actually process. If the money went out, U.S. Treasury is going to make you responsible for it because you were supposed to be acknowledging the sanction programs.

On top of that there are civil monetary penalties that they've imposed in particularly egregious cases. Fintechs need to carefully think about how -- whether they are making payments, lending, handling digital assets and crypto – how someone could exploit their system to bypass the sanctions. We've seen it happen. In Venezuela, following the contested 2015 election when President Nicolás Maduro was supposedly reelected, the U.S. implemented very aggressive sanctions programs. Venezuela turned to cryptocurrency to bypass them. If you were operating an Air France flight and you landed in a Venezuelan airport, your gate fee, your fuel bill, everything was paid in Bitcoin, because that fell outside the U.S. sanctions programs. We've seen even small fintechs in the U.S. being used to launder funds and Bitcoin that was obtained by the Venezuelan government. These were tiny programs which the Maduro government realized were likely to have the least robust anti-money-laundering and sanctions compliance infrastructures.

This is all going to throw a lot of monkey wrenches into many business dealings. I'm assuming there are going to be disputes as a result. What kind of litigation do you anticipate coming because of these sanctions?

You are going to see a lot of people trying to invoke force majeure clauses or terminate contracts that may touch on transactions with the Russian Federation.

A lot of companies are looking at company policy and ethics policies to determine if they can continue these transactions. A number of large companies have been just terminating contracts. An offshoot of this will occur. Take something as simple as Starbucks terminating its contracts in Russia. Are they also going to terminate their shipment contracts in the U.S. for the companies that were shipping Starbucks coffee into Moscow? It's going to impact suppliers in the supply chain.

You also mentioned cyber-attacks. Do you anticipate litigation there?

This is concerning for insurance companies that insure fintechs for cybercrime, cyber liability, or other types of general professional liability. Most of those contracts are not very specific about undeclared wars between nations. If for some reason my data is hacked in the Ukraine, is that covered? To what extent is it covered? Is that part of a declared war? Will our general cybercrime policy protect that data? What if we're sued by vendors for terminating contracts because of business ethical guidelines, but not because the U.S. government forced us? Is that now an insurable event? You might voluntarily take on a liability that the government didn't make you take on, because you can still transact business with people in Russia as long as they're not on the list. You would have to make that choice. You may be sued for not engaging in that contract because you made a choice on your corporate ethics policy not to do business with Russian nationals.

Any resolution of these things takes a long time. The U.S. froze billions in Iranian assets in 1979 after revolutionaries stormed the American Embassy and took 52 American hostages for 444 days. An agreement was reached that included referring monetary claims to a special tribunal. It took until 2014 to resolve all private claims.

This does not move fast. With OFAC, if something is blocked, the only way to unblock it is to seek a "license." You apply to the Treasury for this and make case that you have a legitimate transaction. There are licenses right now in Ukraine to send medical supplies and certain foods. But it can take years or up to a decade to get a license for a particular transaction. And, to your point, sometimes just the time that expires kills whatever the benefit is.

In closing, what must fintechs be doing right now?

The two immediate questions you've got to answer are: First, have you implemented a screening program? And have you ingested these OFAC sanctions for your own customers, meaning are you actually following the sanctions? Second, if you don't have that, you need to immediately assess your vendors and determine which of them may have exposure to Eastern Europe or Russia where there could face potential cyber liability risks.

Then, if you don't have a corporate ethics policy, it's important that you think about how your company is going to respond to these programs. You want to establish your company's position so that you're not figuring it out in crisis mode. Everyone might say, "Yes, stop all business with Russia." Everyone will say, "Absolutely. We support it."

But make sure you're thinking carefully about what that means for your business what that impact is.

When we look at the long-term actions. You've got a much longer horizon to think about as you do your offshoring. As you continue to do the infrastructure build for your fintech, do you want to avoid certain regions that carry a high risk of being embroiled in regional conflicts? Eastern Europe being a prime example. If you're using Taiwanese programmers, or Hong Kong or Singapore programmers, obviously there are questions about how China's going to respond to a lot of this. Are they going to make additional plays to act against either these former British protectorates or, obviously, the disputed Taipei, Taiwan situation? How companies will handle their outsourcing is something they need to address.

Brad, thank you very much for talking to me about this. It's an important subject.

Absolutely. It's been a pleasure.

Based in Greenville, South Carolina, Brad Rustin chairs the Financial Services Practice Group at Nelson Mullins Riley & Scarborough. You can reach him at Brad.Rustin@NelsonMullins.com.