Lowenstein Sandler's Cybersecurity Awareness Series
Session 7 - Understanding the Additional Risks When Making a Ransomware Payment

By Doreen M. Edelman, Christian C. Contardo, and Ken Fishkin
JULY 2022

Ken Fishkin: Hello, and welcome to another episode of Lowenstein Sandler's **Cybersecurity Awareness series**. I'm Ken Fishkin, the Manager of Information Security here, and today our guests are at Lowenstein's Washington, D.C. office. We have Doreen Edelman, the Chair of our Global Trade & National Security practice, and we also have Christian Contardo, who is an attorney for that practice, and he comes with 15 years' experience working as a national security legal advisor for the departments of DHS, Treasury, and Justice. And their practice really focuses on the intersection between trade, national security, and technology.

Now, the reason why I want to speak to these two guests is because ransomware is the biggest cyber threat right now. And a lot of people—a lot of organizations, I should say—think that the ransomware payment is the only thing that they have to be worried about, when in reality, if they're dealing with a country that is sanctioned, or an entity that's sanctioned, there might be additional penalties.

So my first question is for Doreen: what are the other financial penalties that one might face when dealing with a ransomware payment?

Doreen M. Edelman: Well, thanks Ken for having us, because we see this as an important topic and something that comes up when companies don't have a lot of time to think about the next step. So the concern is that if the attacker happens to be on one of the Treasury Departments'—Office of Foreign Assets Controls, commonly called OFAC—on any of their lists of restricted parties, a U.S. person can't do business with that party. So on top of paying the ransom, the party then is open to a penalty from the Treasury Department if the attacker is actually an entity or an individual on the list. U.S. persons, wherever they are, have to comply with U.S. sanctions and its strict liability, which means even if the company hit with the ransomware attack is not aware of these laws and regulations, they still can be hit with the penalty. The penalties can be criminal or civil; if they're civil, they're about $330,000 for each violation, and they can add up quickly.

Christian, do you want to mention about the policy, the cybersecurity policy?

Christian C. Contardo: Thanks Doreen. I think it's also, it's not just specifically identified people on these lists; it's also going to be actors from embargoed regions like Iran or Cuba, North Korea, and they may not be on a list, so it can be a little more difficult to determine if there's a sanctions issue in the transaction. But it's also, I think, important to note that OFAC has been looking at these issues for a while; there's been a cybercrime sanctions program specifically targeting cyber actors since 2015, and OFAC's been publishing guidance more recently on compliance and cryptocurrency, and dealing with ransomware where they're really encouraging companies to go forward when they're attacked and have a ransomware situation and let OFAC know, and let other U.S. government agencies know, so they can try and combat these issues.

Ken Fishkin: All right, okay, that sounds reasonable. Now we all know that there are some companies that really just don't want to get the government involved if they were to get hit with a ransomware attack. They just want to keep it quiet; they don't want to make it public. Do you have any advice for those companies, the ones that just really want to pay the ransom?

Christian C. Contardo: That is definitely an option. I think we would advise companies to take a hard look at their situation—every situation's unique—and make an appropriate business decision. There's risk in not disclosing to OFAC, but there's risk in making a disclosure as well. If you don't disclose, you know, the opposite of what I said earlier is that OFAC will consider your lack of disclosure an aggravating factor in any penalty assessment, so it could count against you if you don't disclose and OFAC finds out separately. They also publish settlement agreements with companies, and if you didn't disclose, that would be noted in a settlement agreement that's made public, and so, you know, a company could face reputational issues as a result of that. On the other hand, even if you disclose and you cooperate with OFAC, they look at the totality of the circumstances in every case, and they may still determine that there's a financial penalty if that's appropriate in a particular case, so you're not guaranteed to get off scot free if you just make a disclosure.

Doreen M. Edelman: So it's a business judgment, and the company needs to document its decision; at least in my opinion, I would suggest they do that in case OFAC does come if they don't make a disclosure.

Ken Fishkin: Well thank you Doreen and Christian for discussing this topic with me today. I'm sure it was enlightening for our viewers as well. Please stay tuned for future episodes. Thank you very much.