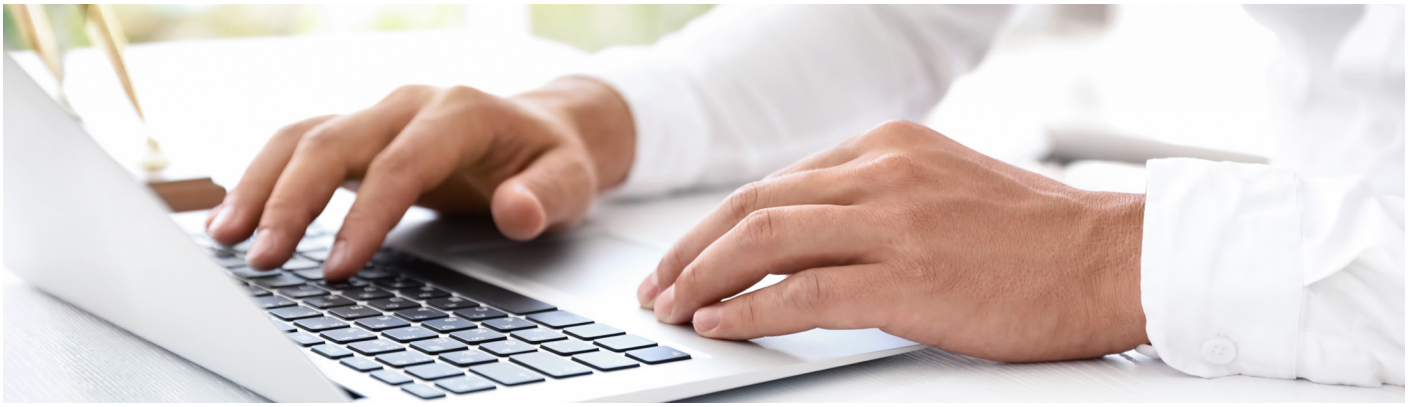
# Zurich North America: Guidance on OFAC Ransomware Advisory



## Compliance risk associated with ransomware payments and impact to the insurance industry.

On October 1, 2020, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") issued an advisory ("Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments") to highlight the sanctions risks associated with ransomware payments related to malicious cyber activities.

Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, may risk violating OFAC regulations in addition to the risk of violation that the victim is exposed to for making a ransomware payment to subjects on the OFAC sanctions list.

The advisory cites increases in reported ransomware attacks reported by the Federal Bureau of Investigation's Internet Crime Reports as cause for concern. The reports cite a 37% annual increase in reported ransomware cases (and 147% annual increase in associated losses) from 2018 to 2019. In response, the OFAC Advisory aims to provide guidance on regulatory risks arising in the aftermath of a ransomware attack. While the advisory does not create any new requirements, it serves as an important reminder of the potential sanctions risks to insureds and insurers and highlights the relevance of OFAC to the insurance industry in the context of cyber protection insurance products.

OFAC sanctions programs generally prohibit U.S. persons from engaging in transactions, directly or indirectly, with individuals or entities on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List), other blocked persons, and those covered by comprehensive country or region embargoes (e.g., Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria). As a general matter, OFAC enforces sanctions under a strict liability regime. This means that any U.S. person participating in or facilitating a prohibited transaction may be subject to an OFAC enforcement action.

Criminal penalties include a fine of up to $1 million and/or up to 20 years in prison for each violation. Civil penalties include a fine of up to $55,000 for each violation. Other penalties for violations of OFAC regulations include seizure/forfeiture of the goods involved.

By providing the information herein, Zurich does not undertake to provide legal advice of any nature nor establish an attorney-client relation between any person and Zurich. Rather, when faced with a ransomware payment demand, Zurich strongly recommends the insured obtain independent legal advice to ensure that the insured's payment of ransom is legally permissible, and that the insured may make a payment without encountering the substantial criminal or civil penalties identified above. Insureds should undertake a variety of actions to ensure avoidance of OFAC criminal fines and penalties, and other civil remedies. While insurance coverage may be potentially available to reimburse an insured for a ransom payment, insurance coverage is not protection from OFAC sanctions.

Victims of ransomware attacks are encouraged to retain expert legal and technical assistance and to contact OFAC immediately to evaluate whether a request for a ransomware payment may involve a sanctions nexus. Victims should also contact the U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection if an attack involves a U.S. financial institution or may cause significant disruption to a firm's ability to perform critical financial services. In fact, OFAC has stated that it will consider a self-initiated, timely, and complete report of a ransomware attack to law enforcement as well as full cooperation with law enforcement during and after the attack as significant elements of its evaluation of actions taken in response to a ransomware attack.

## Zurich affirms commitment to customers, and compliance with laws and regulations, including sanctions programs administered by OFAC.

In keeping with OFAC guidance, Zurich has in place a comprehensive, risk-based Compliance framework. This framework protects Zurich from any action which would violate applicable trade or economic sanctions law or regulation. This program is commensurate with the Zurich Sanctions Exclusion Endorsement which articulates that Zurich will not, "Provide coverage nor will we make any payments or provide any service or benefit to any insured, beneficiary, or third party who may have any rights under this policy to the extent that such cover, payment, service, benefit, or any business or activity of the insured would violate any applicable trade or economic sanctions law or regulation."

Ransomware payments are subject to elevated compliance risk due to circumstantial lack of information on the identity or location of the malicious actors. Enhanced due diligence steps are necessary to uncover this identity, and location, as part of a risk-based compliance program. Accordingly, prior to indemnity payment(s), malicious ransomware attacks are subject to enhanced due diligence steps which are designed to verify, and screen (against sanctions listings), the identity and location of the malicious cyber actor.

This includes:

1. Disclosures to customers, upon receipt of request for consent to cyber ransomware payments, which reiterate the Zurich Sanctions Exclusion Endorsement, and informs the insured on the obligation to:

   a. Provide information, to Zurich, in order to enable independent evaluation of compliance with Laws including OFAC. This may include transparency on steps taken by the customer to uncover the identity of the malicious cyber actor; and

   b. Inform Law Enforcement that a criminal event has occurred.

2. As part of this disclosure process, Zurich will evaluate the need to conduct an independent investigation, separate and apart from the customer's investigation, and law enforcement notification.

Throughout this process Zurich will continue to coordinate closely with its Insureds to deliver on its commitments, and contractual obligations, while doing so in a manner which complies with relevant trade and economic sanctions.

Zurich
1299 Zurich Way, Schaumburg, IL 60196-1056
800 982 5964 www.zurichna.com



A1-112014084-A (12/16) 112014084

ZURICH®