Crime trends during COVID-19: how to safeguard your business 2/19/20

Amid the international outbreak of COVID-19 and the resulting public uncertainty, we see that crime in general, including fraud, blackmail, money laundering and other economic crime, tends to grow. It basically makes sense to expect such activities from persons that have been involved in illegal activities and tried to exploit the weakest links of the existing legal framework and public order in their own interests. A similar illegal strategy is implemented in the present situation, in which people are focusing on other crucial and urgent issues and becoming less cautious or making rash decisions because of the emergency situation. Practice also suggests that the rising crime rates are directly linked to the circumstances caused by COVID-19.

What international organisations have observed

International law enforcement organisations (including INTERPOL and Europol) offer an overview of crime trends and have identified key threats, including:

- A significant increase in threats related to cybersecurity, such as malicious domains, malware or ransomware;
- Targeted attacks on providers of medical and health services and on distributors of goods crucial to health care as critical elements of infrastructure;
- Fraudulent trading and forgeries in the distribution of personal safety equipment and antivirus medicines;
- Increased trade in illegal intoxicating substances through social networks, encrypted apps, or the darknet;
- Individuals and businesses suffering from a significant reduction in income may fall victim to lenders financed by organised criminals charging exorbitant interest rates.

The Financial Action Task Force, too, notes the spread of various criminal activities, such as various types of fraud, raising funds for fake charitable organisations, advertising false medical aid or equipment, offers of fictitious investment opportunities, and various phishing methods. Regulatory and law enforcement agencies are urged to continue providing informational support to the private sector, explaining the significance and potential impact of the present situation on how organisations operate. Businesses need to pay more attention to threats caused by COVID-19 related to money laundering, especially assessing the possibility of fraud involving crime and terrorism financing.

We encourage you to explore the findings of PwC's Global Economic Crime and Fraud Survey 2020, which reflects the global crime trends before the emergency situation was declared.

AML/CTPF risks

Persons subject to the AML/CTPF Act should now be particularly cautious and, in addition to typical risk factors, evaluate the circumstances caused by the emergency situation and how they affect their customers and suppliers, financial or other types of transactions, internal control systems, and related risk management mechanisms.

During the emergency situation, our focus should be on the following factors:

- Unusual activities on the part of customers and suppliers;
- Establishing new business relationships (conducting due diligence reviews and tightening up further supervision);
- Seemingly advantageous terms for a transaction or business;
- Suspicious and complicated transactions;
- Any deviations from the normal activities of customers – in income levels, legal or accounting solutions, services used, and business conducted, as well as small-scale financial transactions.

In monitoring changes to the social and economic environment, businesses also need to evaluate how to best adapt their risk management and control mechanisms, and decide, if necessary, to introduce new elements to their internal control system in order to fight any threats caused by the emergency situation. When evaluating the circumstances and the company's business characteristics, the following areas should be critically evaluated:

- the structure and functionality of the company's internal control system, including methods used for managing certain risks;
- the need to revise or assess the company's AML/CTPF or sanctions risks;
- the company's IT system infrastructure, security settings and functionality, including an assessment of business continuity, information storage, data analysis and management mechanisms;
- findings of internal audits or external expert reviews and performance of the turnaround plan, if necessary revising it and evaluating the significance of recommendations to be implemented;
- the company's management model and organisational structure, including the rights, obligations and operational conditions of certain functions.

Remember that risk management practices that you put in place early and carefully will safeguard you from the effects of illegal activities, operational limitations and potential legal or financial complications, as well as ensuring efficient business operations in the emergency situation.