Fintechs must stay compliant in aftermath of Covid-19 (3) (3/29/20)

This article completes what we wrote last week (03.07.2020; 10.07.2020).

Requirements of the Anti Money Laundering and Counter Terrorism and Proliferation Financing Act ("AML")

Background	• AML applies to all financial institutions and virtual currency service providers. • AML subjects with branches or legal representatives operating in another member state must ensure that those branches and legal representatives comply with the member state's national AML requirements. • The company must appoint a member of the board responsible for AML. • It is advisable to obtain a statement that the company's board members do not have a criminal record and to document their reputation in the company's system of internal controls.
Mitigating internal threats	Staff breaches due to relatively easy access to customer information, remote working, or access to sensitive information
Policies and procedures	• Determining the risk appetite • The obligation to set up a risk assessment system with internal controls • The policy does not need to be a "dissertation." • Procedures are all about "what needs to be done and how we do it." • A single policy and procedure document is not a solution.
Availability of compliance information to AML subjects from Latvian information systems	To perform its obligations, the company may request and receive* entries and details of shareholders and beneficial owners from the Latvian Enterprise Registry and to store and otherwise process this information to evaluate details of customers and their business partners and the need to report a suspicious transaction to the Financial Intelligence Unit or to refrain from entering into a suspicious transaction and to find out whether the customer has started corporate insolvency proceedings or legal protection proceedings. * *For a fee – entries from the State Revenue Service's registers, the Penal Register, the Single National Computerised Land Register, the National Register of Vehicles and Drivers, and the Population Register*
Risk assessment	• Customer risk – new customers making substantial one-off transactions and having complicated ownership structures • Product and service risk – the ability to move funds around quickly • Residence/registration country risk – forged ID documents • Supply channel risk – increased potential for anonymity
KYC (Know Your Customer)	• Improved and resistant ID and verification apps • Metadata review to verify authenticity of scanned documents • Interactive interfaces

Customer supervision	• Sanctions list • Politically exposed persons (PEPs) • Negative media • Using a manual + automated verification approach
Sanctions	The National and International Sanctions Act requires the company to conduct and document a national and international sanctions risk assessment in order to identify, evaluate, understand and manage the risks of non-compliance with national and international sanctions imposed on their activities or customers.
Training	The company must ensure that its staff in charge have a good knowledge of AML legislation, and must provide regular staff training to improve their ability to detect suspicious transactions and recognise their signs.
Reporting	• Each suspicious transaction must be immediately reported to the Financial Intelligence Unit. • The duty of notification extends to any funds arousing suspicion that they have been directly or indirectly obtained as a result of any criminal activity or are linked to any actual or attempted terrorism and proliferation financing. • Any reports filed with the Financial Intelligence Unit must be recorded and made available to supervisory and control bodies on the next working day.
Recommendations	• Decisions on the risk appetite, resource allocation and technology should be made at management level. • Resources should be efficiently managed and risk mitigation strategies adjusted. • AML should be seen as part of the business and not as an obstacle.
Penalties	A fine of up to 10% of total annual turnover (or at least EUR 5 million), including a fine on the officer, staff or person responsible for performing a specified activity at the time of the breach, up to EUR 5 million