COVID-19 Managing financial crime risks

April 2020

The COVID-19 pandemic continues to grow with increased impact on the global economy triggering business continuity and crisis management responses across organizations of all sectors and sizes. At the same time, the financial services industry faces new unique threats from fraudsters and continued expectations from regulators that anti-money laundering (AML) compliance must be maintained despite the disruption to business-as-usual.

In addition to addressing the risk of the new fraud typologies, as of March 19, 2020, FINTRAC maintained its expectation that regulated entities, including banks and other financial services companies, should do everything possible to meet all of their obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) and associated regulations. In a situation where regulated entities are unable to meet some of their obligations, FINTRAC is requesting that the reasons be documented and maintained. FINTRAC states that when it comes to reporting, priority should be given to submitting suspicious transaction reports (STRs).

KPMG's Financial Crime services team can assist with fraud risk management, providing short-term resourcing, virtual training, forensic data analytics, and technological solutions to assist in mitigating the risk of financial crimes during these challenging times, while striving to ensure timely compliance.

Key considerations for effectively managing financial crime risks during COVID-19

Key considerations	Ask your organization	Potential response strategies
Maintain culture of compliance with virtual teams	- Does my organization have the technological capabilities to handle a large number of employees now working remotely? - Are my teams able to conduct their compliance responsibilities (KYC, TM/Sanctions alert review, Investigations) effectively to ensure compliance with regulatory requirements? - If company devices are being used from home, are cybersecurity and sensitive information risks being adequately addressed?	- Consider the impact on compliance, productivity and cybersecurity of using various technology solutions available. - Leverage technological solutions to provide virtual training on new fraud and AML typologies, as well as on revised digital processes from the manual, paper-based processes which are no longer feasible.
Added workload with short term loan applications	- Does my organization have processes in place to screen short-term loan applications? - Does my organization have the capacity to process the volume? - Does my organization have the capacity to onboard clients virtually?	- Consider your resource requirements for the short-term loan application process. - Create, document and deploy new technology-based processes for handling these applications. - Assess your methods of onboarding to ensure they meet regulatory requirements.

© 2020 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

New COVID-19 fraud typologies	- Are my employees and customers aware of the new fraud typologies such as COVID-19 themed phishing attempts that can result in theft of personal data to enable account takeover, credit / loan fraud, card not present fraud, payment diversion fraud, among many other deception schemes?	- Provide ongoing and up-to-date training to ensure awareness among employees of the new fraud typologies and actions to be taken in order to prevent and detect them. - Review and/or employ your cyber incident response strategies and if necessary, consider the information security and data privacy impacts. - Ensure your fraud and AML teams are well-connected to ensure timely reporting of suspicious activity to FINTRAC.
Transaction monitoring of changing consumer behaviour	- How is my customer's behaviour changing given the pandemic? For example, is your organization faced with an increased number of cash withdrawals? - Do my transaction monitoring (TM) rules account for deviations from the historical customer profile and could the change in consumer behaviour result in increased monitoring alerts? For example, is your organization faced with increased usage of digital channels by customers to undertake their financial affairs? - How should TM alerts be prioritized based on the disruption to business-as-usual given the regulatory focus on STRs?	- Leverage data analytic insights to understand the new consumer behaviour and segment high risk profiles for closer monitoring. - Re-assess TM models to appropriately capture the new risks posed by new COVID-19 related fraud typologies. - Consider your resource requirements for the potential of an unexpected surge in monitoring needs.

Contact us

Hitesh Patel
Partner, Forensic
National Co-Lead Financial Crime
416-777-8191
hiteshpatel2@kpmg.ca

Éric Lachapelle
Partner, Forensic
National Co-Lead Financial Crime
514-840-8365
ericlachapelle@kpmg.ca

Rebecca Ip
Vice President
Forensic and Financial Crime
416-777-3257
rip@kpmg.ca

Dominic Hurtubise
Executive Director
Forensic and Financial Crime
514-840-8369
dhurtubise@kpmg.ca

Janice Mensah
Executive Director
Forensic and Financial Crime
416-777-3365
jmensah1@kpmg.ca

Steve Fantham
Senior Manager
Forensic and Financial Crime
416-777-8061
sfantham@kpmg.ca

Mélanie Gagné
Senior Manager
Forensic and Financial Crime
514-940-4382
mgagne@kpmg.ca

© 2020 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International.