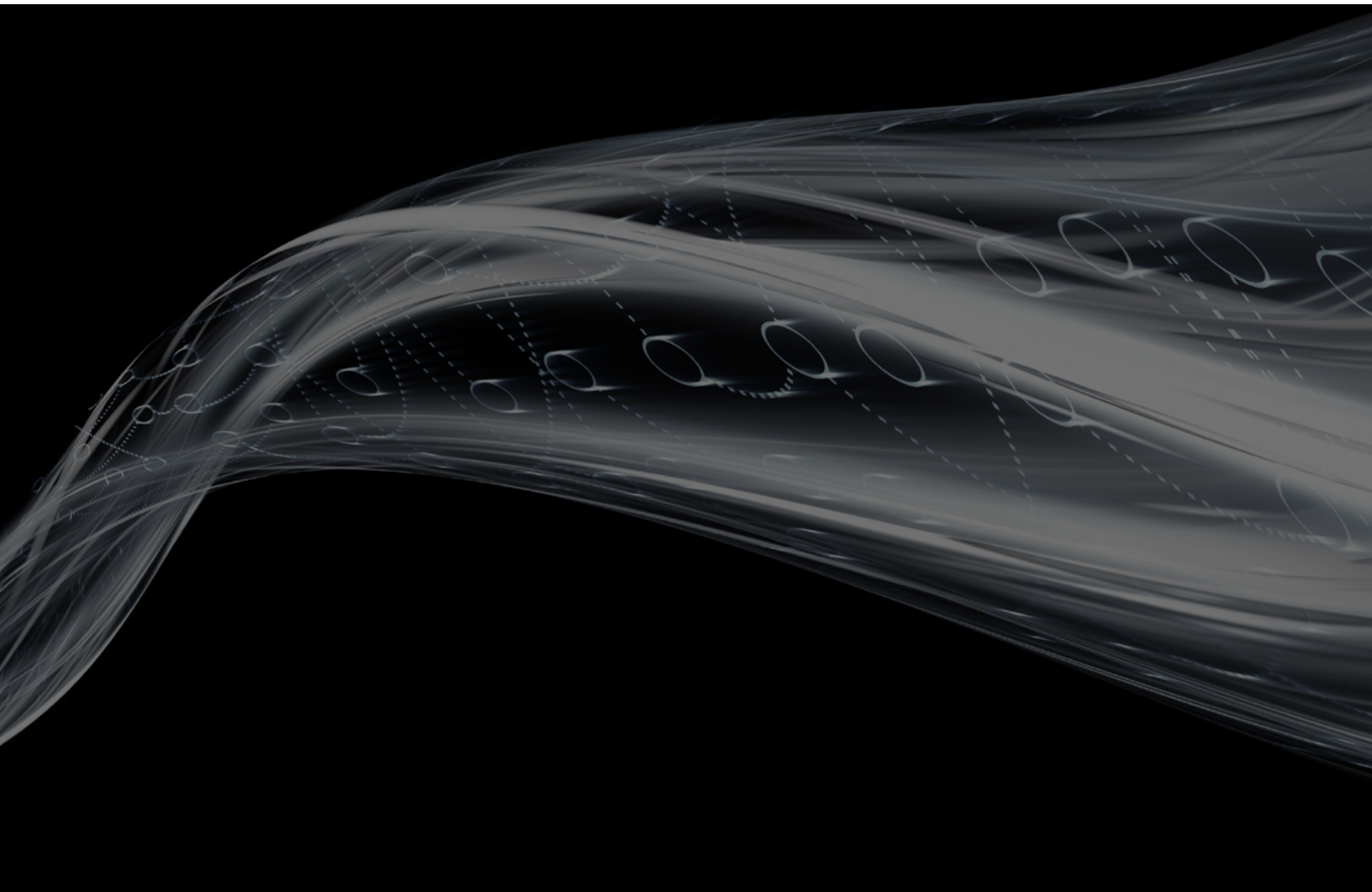
CAPCO

MANAGING A REMOTE FINANCIAL CRIMES COMPLIANCE PROGRAM DURING COVID-19



INTRODUCTION

Global impacts of COVID-19 have accelerated a digital movement and remote working model for some elements of an anti-money laundering ('AML') and sanctions compliance program that likely was already in motion.

In the context of the current pandemic, financial institutions globally are facing significant challenges due to:

1. A convergence of (probable) increased criminal activity and fraudulent schemes seeking to capitalize on the pandemic

2. The strains of a remote workforce

3. A decrease in staffing capacity, and level of timely communication required to run an effective AML and sanctions compliance programs (i.e., a stale AML business continuity plan ('BCP')

4. Changes in customer behavior – namely the ability to pay none, or only a fraction of critical bills such as mortgage payments, rent, auto loans, and credit cards

Similar to the financial crisis of 2008, the current pandemic is likely to see additional elements of fraud in many areas of the financial services industry as investors and families attempt to gain access to their funds, only to discover that they were misappropriated before COVID-19. However, the current pandemic introduces new fraudulent activity cases, namely around the misuse of government bail-out funds. These new cases are happening precisely at a time when many financial institutions are struggling to maintain pre-COVID activities, and when regulators are emphasizing the continued importance of financial crimes compliance.

This article highlights certain components of an AML and sanctions compliance program, where we have seen an acceleration in response to COVID-19, articulates associated risks, and suggests potential solutions to maintain program effectiveness. Capco believes the current pandemic highlights the need for financial services to increase investment in technology to meet the accelerating needs of its online customer base, remain competitive, and meet compliance obligations.

COMPLIANCE PROGRAM IMPACTS

1. CLIENT ONBOARDING

Significant challenges may arise during account opening, especially for financial institutions that do not have online/remote account opening processes. Such institutions will be forced to adapt their products to reflect that customers may not wish to enter a branch to open an account.

Additional challenges concerning the customer identification program ('CIP') and associated customer due diligence ('CDD') documentation and verification process will be disrupted as document hard copies may be inaccessible remotely. There may be reliance on crucial information from third parties – namely related to beneficial ownership documentation – who are also navigating the effects of the pandemic.

Finally, critical metrics, such as a customer's expected versus actual activity, may no longer be relevant as people's lives, businesses, and behaviors were altered by COVID-19. Typically, this data is updated as part of risk-based know your customer ('KYC') updates (or periodic 'refreshes'), or routine transaction monitoring and investigation activities. However, financial institutions must weigh the effects of COVID-19 on their KYC refresh programs and determine how 'risk-based' applies in this context.

Banks lending to small businesses participating in the Paycheck Protection Program ('PPP') under the CARES Act will need to ensure that CIP and other elements of KYC and onboarding are performed quickly, but without sacrificing regulatory compliance. The loan recipient will want to receive the much-needed financial aid as soon as possible; however, an inefficient KYC process could lead to delays in loan disbursement or restrict the application process to existing customers. Banks will need to examine their ability to perform 'expedited KYC' for SBA loans, a process that is likely already slowed by remote people and processes.

Global Focus: APAC

- In Asia, the Regulators issued formal announcements pre and post FATF statement published on April 1, 2020, that encourages the full adoption of digital customer onboarding and delivery of digital financial services in the light of social distancing measures. The Hong Kong Monetary Authority (HKMA) subsequently encouraged the adoption of fintech that will bring significant opportunities in managing the current social distancing needs in the customer onboarding process. Across Asia, there is still a rising number of customers unfamiliar with online platforms that impose technology constraints on FIs.

- The HKMA expects FIs to adopt robust technology solutions for remote onboarding compared to when the customer is in front of the FIs staff, ensuring two aspects:

    1. The authenticity of the customer's identity to ensure the reliability of the information obtained in the form of the document, image, or other data form
    2. Identity verification – FIs should use appropriate technology (e.g., biometric solutions and liveness detection) to link the customer incontrovertibly to the identity provided in (i). It is often debated that use of technology solutions for digital KYC brings more benefits compared to the in-branch checks (e.g., it's easier to detect scams when high-end smartphone camera is used for customer identification compared to eyeball test)

- The Monetary Authority of Singapore (MAS) announced a relief fund and support package for the financial and fintech sectors to deal with the immediate challenges from COVID-19 and position strongly for the recovery and future growth.

- The Indian securities regulator encouraged technology adoption for AML compliance in the investor KYC process, using video-based ID verification, liveness checks, e-signatures, and scanned documents for registration renewals.

- Asia is growing at a remarkable pace in the digital banking space. Eight virtual banking licenses were issued in Hong Kong in 2019, while five in China since 2014. Singapore's ambition was to issue five new virtual banking licenses last year (postponed beyond June 2020 due to pandemic), and South Korea has issued three licenses so far.

Global Focus: UK

Recent statements from the UK Financial Conduct Authority (FCA) reaffirm their commitment to maintaining the integrity of the financial market, even during the severe operational challenges of COVID-19.

Some minor relaxations on standard approaches to client onboarding have been allowed. However, there's an emphasis that the rules remain in place and any flexibility is within the principles that:

1. Firms must continue to operate within the legislative framework
2. Any changes to operations are 'reasonable' and on a risk-basis

For client onboarding, the FCA directs firms to the existing money laundering regulations and Joint Money Laundering Steering Group (JMLSG) guidance for verifying customers remotely. Highlighted options to support verification include:

- Accepting digital photos or videos, or scanned documents (preferably PDFs)
- Verify phone numbers, emails, and/or physical addresses by sending codes to the client's address to validate access to accounts
- Using reliable third-party verification or commercial providers to triangulate multiple data sources to corroborate verification

You can find additional guidance for non-face-to-face identification and verification issued by the Law Society during COVID-19 here.

For Customer Due Diligence (CDD) and periodic review, the FCA has allowed for some re-prioritization or reasonable delays to CDD checks. However, like above, the 'reasonable' test is firmly contextualized within the firm's existing legal obligations, consideration of the firm's risk appetite and the risk profile of the client, and the requirement that a clear 'plan to return' to normal review be in place.

'High-risk' activity controls are expressly excluded – with counter-terrorist financing controls and timely Suspicious Activity Reports (SARs) as having no relaxations.

Overall, even during this public health crisis, the message for firms is that they continue to focus on meeting their obligations - including not addressing the operational challenge by changing their risk appetite or weakening the effectiveness of their controls. This message continues the emphasis from the FCA on operational resilience made in other guidance and the Business Plan 2019/20 published last April.

You can find the FCA detailed guidance to help firms fulfill their Financial Crime Systems and Controls (SYSC) obligations during COVID-19 here. The statement highlights Customer Due Diligence (CDD) requirements explicitly and recognizes that restrictions on travel and the closure of branches may hinder a firm's ability to verify a customer's identity. Additionally, it refers to the application of an alternative and pragmatic approach. However, regulators are steadfast that firms must continue to comply with the regulations.

Global Focus: Germany

As is the case within the US, UK, APAC, and the rest of Europe, COVID-19 has accelerated the switch from a more traditional, paper-based onboarding process to a digital one. Although most banks and lenders can accommodate remote onboarding processes, there are still significant hurdles when onboarding processes rely upon paper documentation – especially with corporate customers.

COVID-19 relief packages distributed by German banks have faced similar challenges to other financial hubs. Financial institutions are having difficulty identifying and preventing new types of fraudulent activities associated with relief funds —especially regarding smaller loan amounts. One factor is that lending activities must be allocated quickly, creating a backlog of financial crime compliance checks, accentuated by an increasingly remote compliance workforce.

German financial institutions also face customer segmentation challenges because of COVID-19. Traditionally, segmentation is performed during onboarding to allow the proper cadence for ongoing transaction monitoring; however, new customer behavior and remote client onboarding have significantly hindered this step.

Many compliance functions have adopted an agile or scaled agile response to address the challenges presented by COVID-19. Which, in turn, has impacted many German financial institutions' risk-based approach to financial crimes compliance. As a result, many banks are leaning heavily on their audit function to support the compliance function's integrity.

2. CURRENCY TRANSACTION REPORTS ('CTR') AND SUSPICIOUS ACTIVITY REPORT ('SAR') FILING

Due to the remote nature of their workforce and potential drains on compliance staffing capacity, financial institutions will see significant challenges in meeting certain BSA obligations. These challenges include timing requirements for certain report filings, as their people, processes and technology become remote. Although FinCen recently stated, "it recognizes certain regulatory timing requirements with regard to BSA filings may be challenging during the COVID-19 pandemic and that there may be some reasonable delays in compliance," they only offered a narrow form of relief in the form of CTR obligations for an even more narrow class of entities[1].

Global Focus: APAC

- In Asia, several regulatory initiatives have been deferred due to the COVID-19 crisis. For example, the NZ government issued a list of amendments bills (financial markets infrastructures bill, fair trading amendment bill, credit contracts regime, etc.) deferred to later dates. MAS SG has delayed the virtual banking license award to 2H 2020, instead of June 2020. APRA, the Australian regulator, announced two prudential standard reporting dates to be delayed by around one year.

Global Focus: Germany

- The German regulator (BAFIN) is not planning any form of COVID-19-related relief from meeting regulatory obligations.

1. Id.

3. TRANSACTION MONITORING PROGRAM

During this COVID-19 outbreak, financial institutions may see a surge in their transaction monitoring alerts due to: (i) a likely increase in criminal activity; and (ii) also increases to (and deviations in) transaction activities from a worried customer base. Remote BSA/AML compliance teams may be operating with fewer resources and less coordination than before. Therefore, transaction monitoring rules must be reviewed (and recalibrated where possible) to reflect a bank's highest risks and consider the efficiency of alerts that systems have previously produced. The term 'risk-based approach' concerning transaction monitoring programs has never been more meaningful.

Financial institutions will not want their BSA/AML staff to become overwhelmed by alerts generated from customers deviating their transaction behavior in response to COVID-19. Instead, the focus should be on identifying actual criminal activity, and to adjust monitoring protocols accordingly. Turning off specific alerts altogether without adding additional scenarios could prove risky, as regulators could subsequently question if they missed potential illegal activities when the initial alerts were suppressed. Perhaps a better solution would be to generate all alerts and provide analysts with more time to review them or use a triage approach to prioritize the alerts producing actionable financial crime intelligence.

In addition, business continuity plans ('BCPs') should provide flexibility to compliance programs in times of crisis so that that leadership can make risk-based decisions concerning alert generation. To prevent future confusion, financial institutions should clearly document any changes made to AML and Sanctions programs taken in response to COVID-19, including clear sign-off from senior leadership that the institution has evaluated and accepted the temporary risks presented by any deviation from previous rules.

Global Focus: UK

Priority response for firms should be to utilize external and internal intelligence resources to refine and support their Transaction Monitoring (TM) system rules – and helping them support and to protect their legitimate clients.

- Examples include increasing use of negative news screening and additional key terms to identify clients in financial difficulties that may be at heightened risk of committing fraud.
- Other resources include enforcement agencies, such as the FBI report on increased uses of 'Money Mules' and cash hoarding activity during the disaster, and industry and supranational standards organizations such as the Financial Action Task Force's (FATF) recent report on the increased risk of COVID-19 charity fraud.

Firms will also need to review and document any changes to the TM systems and AML models they use to respond during COVID-19. However, ensuring the documentation and effectiveness testing approach is rigorous and systematic will be vital to getting it right now and in the future.

In July 2017, the New York Department of Financial Services (NYDFS) adopted a yearly requirement for regulated entities to maintain and document *"the reasonableness, effectiveness and relevance"* of their models underpinning their AML and Sanctions controls – NYDFS, Part 504.

In the UK, firms are already expected to be able to readily adapt and refine their TM systems under their operational resilience expectations. However, AML models remain less granularly regulated than Value at Risk (VaR) Prudential Models.

Going forward, referring to the NYDFS standards can help firms design a robust and structured methodology for reliance testing and documentation for their AML-specific data models, assisting them in interacting with regulators effectively and reacting more quickly and consistently to address the next 'new normal.'

Global Focus: APAC

- Many regulatory bodies across the globe have weighed in, calling on institutions to be pragmatic in adopting a risk-based approach to Anti-Money Laundering (AML) compliance in the COVID-19 crisis – for detecting and reporting on suspicious activities. The critical question is whether the 'Business Continuity Plans (BCPs)' of financial institutions for any pandemic situation contain the threshold or rules adjustments.

- As fraudsters/criminals invent new ways for scams in the current crisis and FI staff being attentive more to continue operating in the new normal way, FIs are strongly encouraged to adopt a risk-based approach and remain highly proactive:

    - Transaction Monitoring systems – adjustments are required in the TM systems to avoid an unanticipated surge in alert volume only because of customer's inactivity due to the lockdown constraints. The normal activities will drop off as a natural effect of the pandemic.

    - Adjusting TM systems to limit the alert volume so financial institutions can manage alerts with fewer employees and communicating the same to the regulators – may not be an option for many FIs if not documented in the BCP and approved by FIs risk committee or board. It might be challenging otherwise to get a sign-off on these adjustments from the board about the willingness to accept the risk by deactivating some rules temporarily to avoid generating less efficient alerts.

    - Another alternative to turning off inefficient alerts/fraud rules with a risk of missing a potential illicit activity is adjusting SLAs or policies allowing additional time to the fraud operations team for longer turnaround time on alert responses (board approval needed)

- (II) Behavior Pattern Changes – FIs based the configuration of most fraud rules on a customer's typical spending pattern and behavior. So, for any behavioral-based TM system, in the current situation, it will be important not to detect fraud only by tracking deviations in customer's behavior; but adopting a combined approach along with behavior tracking. Customer spending patterns should be re-baselined according to the customer's current behavior; however, the customer profile maturation process in any TM system takes a while before it starts detecting fraud effectively.

- Some FIs are well equipped to make quick changes to the TM systems, but others may not – this makes those FIs more vulnerable falling prey to the criminal activity.

Global Focus: Germany

Current challenges:

- **The 'new suspicious'** - Financial criminals do not rest during a time of crisis and are trying to develop new patterns to exploit the exceptionality of the situation presented by COVID-19. Financial crimes compliance staff have had to quickly adapt to new patterns of customer and criminal behaviors and have had to do so in a fractured remote working environment.

- **Increase of false positives** - Due to the lockdown, transaction activities linked to restaurants or shops have experienced more than a reduction, while other areas, like cash activities, are experiencing the opposite (a lot of people have been withdrawing cash due to economic fear). These mass behavioral changes could trigger alerts that are not worth being investigated.

- **Staffing** - Many financial institutions have seen a significant decrease in staffing in specific locations over the past weeks, which has affected their ability to review alerts and report suspicious activities to regulators effectively.

- **Organization** - AFC teams who traditionally work on-premise are now working from home. Even if more than 90 percent of FIs can appropriately equip their workforce, the lack of organizational flexibility still affects their efficiency.

Possible measures/some lessons-learned:

- **The importance of governance and technology to adapt** - Some banks may be equipped to make quick changes to transaction monitoring systems. Other banks may not be prepared, but it is essential to identify what is considered the new normal in terms of customer activities and ensure that AFC functions are providing clear directions to analysts.

- **Prioritization and threshold adjustments (instead of turning them off)** - Banks should give themselves more flexibility in terms of when they can look at all of those alerts. The key is prioritizing based on the types that lead to more fruitful outcomes (possibly using ML in parallel).

- **Re-examine the risk-based approach** - From an organizational perspective, this means allocating the workforce differently and introducing (scaled) agile methodologies.

RESPONSIBLE INNOVATION TO MEET BSA/AML COMPLIANCE REQUIREMENTS

In its most recent COVID-19 release, FinCEN encouraged "financial institutions to consider, evaluate, and, where appropriate, responsibly implement innovative approaches to meet their BSA/anti-money laundering compliance obligations, to further strengthen the financial system against illicit financial activity and other related fraud."[2]

Federal regulators have previously stated they welcome a bank's use of artificial intelligence and digital identity technologies – saying they can "strengthen BSA/AML compliance approaches, as well as enhance transaction monitoring systems," including "maximize utilization of banks' BSA/AML compliance resources."[3]

Maximizing a bank's BSA/AML compliance resources without sacrificing regulatory obligations or customer experience is especially relevant. Areas of focus that lend themselves to a digital framework, remote operation and/or third-party outsourcing include the following:

1. Customer Identification Program
2. Sanctions and Politically Exposed Person ('PEP') screening
3. Customer Due Diligence and Enhanced Due Diligence
4. Related beneficial ownership and customer risk-ranking/ ongoing monitoring
5. Alert clearing and case investigations

2. Id.
3. "Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing," Board of Governors of the Federal Reserve System Federal Deposit Insurance Corporation Financial Crimes Enforcement Network National Credit Union Administration Office of the Comptroller of the Currency, December 2018.

If financial institutions choose the COVID-19 pandemic to deploy responsible innovation toward its BSA/AML compliance processes, including blockchain opportunities, there are specific questions that they must answer. These include how to address the security of customer data captured during the account lifecycle, and determining whose security is threatened by possible shortcomings arising from the remote workforce and remote data access.

Customer data used during critical downstream processes of BSA/AML compliance programs, including ongoing transaction monitoring and related alert/case investigation and disposition and suspicious activity reports ('SARs'), must also be accessible to investigators, auditors and regulators alike. Therefore, financial institutions should, at a minimum, determine the following:

- How will KYC data be accessed remotely by critical BSA/AML compliance resources during daily monitoring and investigation activities?
- How will relevant data integrate into existing BSA/AML compliance workflows?
- Where will supporting customer information be stored (e.g., information obtained to verify customer information at account opening)?
- How will event-driven account information be updated remotely (e.g., when beneficial ownership information or expected/ actual customer activity changes)?

Global Focus: UK

As with the FCA's stance on AML legislation during the COVID-19 disruption, a firm's conduct obligations to protect its customers also remain in effect.

With more people staying at home and an increase in both a reliance upon online services and an increase in economic hardship, this has enabled a surge in cyber-enabled and COVID-19 themed fraud – and with it the risks to firms' vulnerable customers.

In response, the UK government has launched several campaigns to protect citizens, highlighting to firms that over £2million has already been defrauded in COVID-19 related crimes since March, and has been used more than any other topic in UK Government-branded scams.

Europol – Catching the Virus

- *The impact of the COVID-19 pandemic on cybercrime has been the most visible and striking compared to other criminal activities.*
- *Criminals active in the domain of cybercrime have been able to adapt quickly and capitalise on the anxieties and fears of their victims.*
- *Phishing and ransomware campaigns are being launched to exploit the current crisis and are expected to continue to increase in scope and scale.*

Source

Examples of common fraud typologies repurposed under COVID-19 include: Text message spoofing for fake payment authorization, email phishing attacks with COVID-19 government support themed scams, and fraudulent companies taking upfront payment and never delivering or only delivering fake versions of critical PPE, masks and hand sanitizer.

Conduct expectations for firms to protect customers from such risks remain in effect, especially for vulnerable customers.

In response, many firms are increasing account controls, for example, around overseas payment limits and increasing follow up customer calls after unusual customer activity.

In parallel, firms are also deploying public information campaigns to educate customers on spotting fraud and employing strict and widely publicized policies around sensitive customer account information – helping reduce the instance and severity of frauds before a customer falls victim.

RETURN TO WORK CONSIDERATIONS

In this US, leading financial institutions have developed a multi-disciplinary approach consisting of crucial operational and control functions, including legal and compliance, which are planning to operate on a rotational basis once they received clearance to return to work. Under this flexible model, financial crime compliance staff will split their support functions between home and the office.

Global Focus: APAC

A phased return to work adoption by many FIs has been observed in Asia. Compliance functions have started operating in a rotation where half of the team supports from office locations, with the remainder still working remotely from home. Developing countries in Asia have had challenges sustaining compliance operations during this crisis, with the same level of effectiveness as before, due to significant infrastructure challenges.

Global Focus: Germany

German banks are planning to come back to the layout before COVID, especially speaking about compliance/AFC functions.

REGULATORY RELATIONS DURING PERIODS OF REMOTE COMPLIANCE

BSA/AML compliance programs operating remotely because of COVID-19 should prioritize communication and engagement with applicable regulators. Periodic check-ins are critical so that regulators are aware of any risk-based modifications a bank may make to its BSA/AML and sanctions compliance programs. For example, banks are currently navigating the new normal relating to customer activity. Transaction monitoring alert rules that produced valuable alerts before COVID-19 may need to be re-evaluated and calibrated; and, custom alerts may be necessary. Given the potential resource shortage and remote nature of compliance functions, banks may need to modify their approach to alert review using a triage or other risk-based method. Providing regulators with necessary updates throughout this remote period on modifications to the BSA/AML compliance program will reduce potential confusion during the examination and allow regulators to comment on the response.

Compliance departments should also be aware of any outstanding regulatory commitments (e.g., MRAs, MRIAs, agreed remedial actions, and results of examination) and how these commitments are affected by the remote nature of the compliance function. Adopting an open channel of communication with regulators, combined with a risk-based approach to remediation efforts, is a more effective strategy than retroactively explaining why certain items were not addressed during an examination. Banks should be able to articulate the effects of COVID-19 on their regulatory obligations clearly, and have a timeline prepared should they require an extension for any agreed-upon remedial action. As FinCEN has not issued any specific and substantial public guidance, banks should proactively maintain an open dialogue with their respective regulators.

Additionally, banks should prepare for the possibility of remote examination for the foreseeable future. Potential challenges regarding a 'virtual' examination process include: remotely coordinating a timely response to regulatory requests involving multiple stakeholders, locating and aggregating required data points from source systems, and coordinating 'deep-dive' conference calls and remote screen-shares with regulators.

Global Focus: APAC

The Hong Kong regulators urged FIs to be more vigilant during crisis time for emerging fraud and ML risks post-eruption of face mask scams in Hong Kong. These risks to be mitigated by informing and reporting suspicious transactions to the Joint Financial Intelligence Unit (JFIU).

Most Asian regulators have offered ongoing support to FIs to maintain normal TM operations to turn around all cases within the agreed timeframe/KPIs. In such cases, to meet obligations in the near-term, FIs are advised to record the current circumstances, risk assessments performed, and any mitigation actions being taken – bringing more transparency to the regulators.

Internal audit functions in many Asian FIs have delayed non-critical audits to the latter half of 2020 to avoid additional pressure on compliance functions, that are operating in BCP mode and also to comply and maintain social distancing measures.

Finally, an efficient and effective governance and change management will be very crucial at this stage to track and document all the changes FIs are making to their TM/AML programs. By documenting these changes for future reference, it helps to avoid confusion and inevitably ensures appropriate communication with regulators.

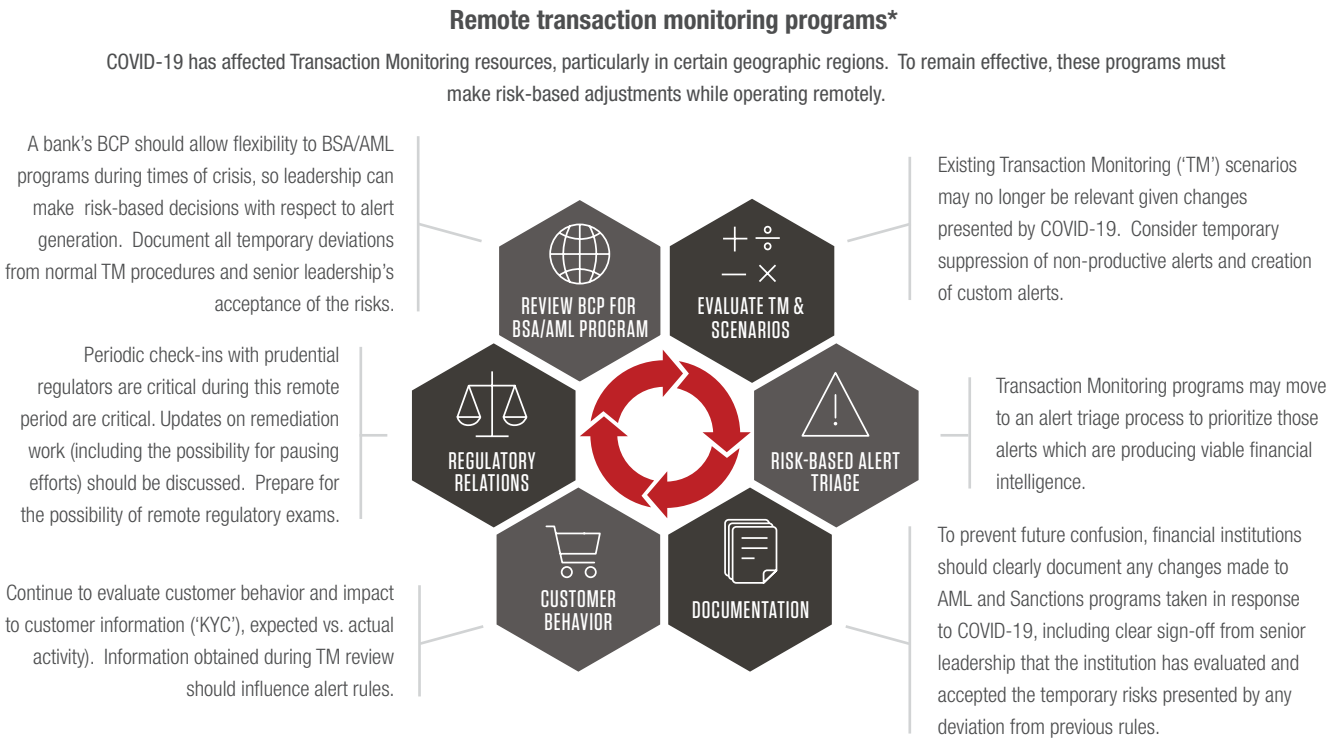
Global Focus: Germany

The importance of an efficient AFC/compliance framework to enhance transparency and efficiency. Banks have to balance their business as usual tasks with their tasks from regulators. This balancing act is an essential aspect to improve relations with BAFIN. For example, due to a lack of transparency and increasing procedural complexity, the German regulator decided in 2018 to install a supervisor at the most prominent German bank (Deutsche Bank), impacting the lender's reputation.

Ensuring open dialogue with regulators and other operators is a must. Anybody operating in this sector should have an open dialogue, especially in the current situation, banks and their compliance teams should keep a careful eye on the developments and sign up to all the regulatory alerts to make sure they're up to date.

The importance of the internal audit function, especially in this exceptional phase, many AFC activities have been partially reshaped, impacting a bank's risk-based approach. A robust audit function must support lenders by improving traceability and decision-making transparency while avoiding excessive future rework and investigation activities.

Fig 1. Managing Remote Transaction Monitoring and Other BSA/AML Functions.



*Sanctions compliance efforts have been similarly affected by remote operations and could also follow the principles listed above in designing a risk-based approach.

AUTHORS

Spencer Schulten, Executive Director
Spencer.Schulten@capco.com

Vipra Kulkarni, Principal Consultant
Vipra.Kulkarni@capco.com

Harriet Roberts, Principal Consultant
Harriet.Roberts@capco.com

Enrico Aresu, Principal Consultant
Enrico.Aresu@capco.com

Geoff Lash, Principal Consultant
Geoffery.Lash@capco.com

Sashi Sekhar, Managing Principal
Sashi.Sekhar@capco.com

Alex Saunders, Senior Consultant
Alex.Saunders@capco.com

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at www.capco.com, or follow us on Twitter, Facebook, YouTube, LinkedIn and Instagram.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Hong Kong
Gurgaon
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO