**Client Alert:**

# Maintaining AML Compliance Vigilance in a Technology Era

JULY 2020


**Emilia Drozda**
Senior Manager, StoneTurn
edrozda@stoneturn.com
+44 (0)20 7427 0409


***By Emilia Drozda***

It is commonly recognized that the rise of global terrorism and changes in public and regulatory attitudes following the 2008 financial crisis have been driving forces behind anti-money laundering and counter-terrorist financing ("AML/CTF") policy and enforcement over the past 20 years.[1] More recently, however, we've seen a series of emerging technology and media developments changing the financial landscape and becoming prominent factors driving the AML/CTF agenda.

## 1 The Rise of Digital Challenger Banks (e.g., Revolut and Monzo)

A major development changing the financial environment over recent years is the rise of digital challenger banks—non-traditional financial institutions with lower fees than more established banks, and no physical branches. Given their convenience and affordability, it's no wonder these mobile app-based banks are attracting more and more users. However, with the premise of a seamless customer experience, and global access, challenger banks face a variety of issues in properly vetting customers during onboarding and ongoing due diligence. Coupled with the challenger banks' relative inexperience in addressing financial crime issues, it has made it easier for criminals to perpetrate fraud by abusing the fast, digital services they provide.



StoneTurn

Due to heavy reliance on technology rather than staff, many challenger bank onboarding processes are relatively hands-off. This can make it easier for malicious customers to slip through the cracks and, in turn, makes challenger banks a prime target for exploitive money launderers. Nevertheless, these alternative banks are required to protect themselves against financial crimes and ensure AML & KYC compliance just like traditional financial institutions. Inevitably, this has resulted in challenger banks being the focus of increased AML/CTF scrutiny in recent years.

For example, Revolut (a British challenger bank with more than 10 million customers worldwide), has found itself in hot water over its AML procedures several times in recent years—from whistleblowers approaching the Financial Conduct Authority over inadequate compliance systems concerns[2] to mistakenly freezing customer accounts for as long as six weeks.[3]


## Increasing Popularity of Virtual Currencies

As virtual currency adoption continues to gain popularity globally, the number of alternative currencies is now in the thousands and regulators are increasingly struggling with the AML risks they pose. Due to its ability to be used for fast, often anonymous international transactions, cryptocurrency has become a modern means to transact proceeds of crime. For example, on one former black-market Internet platform "Silk Road" (where illegal goods or services were offered), Bitcoin was the only means of payment accepted.

Online cryptocurrency exchanges are required to meet varying levels of compliance with AML/CTF regulations, depending on the jurisdictions in which they are incorporated and operate. Reputable exchanges are AML compliant and follow strict regulatory requirements for verification of identity and sources of funds. The vast majority of the Bitcoin trading exchanges both in the US and the UK require some sort of customer ID verification, and a recent study by Elliptic found that less than 0.5% of Bitcoin transactions were used for illicit purchases in 2019.[4]

However, some (often unregulated) exchanges offer less compliant environments for potential money launders. In 2018, a CipherTrace[5] study revealed that 97% of direct Bitcoin payments from criminals went to poorly regulated cryptocurrency exchanges in countries with weak AML/CTF laws. Regulations used to obtain a record of customers and transactions for cryptocurrency ATM machines also differ by country and are often poorly enforced leaving loopholes for criminals to exploit.

Hugely popular online games, such as Counter-Strike and Fortnight, have also been identified by criminals as a means to liquidate their gains, since money launderers can buy in-game currency or virtual items. They then sell these to unknowing gamers through a variety of online marketplaces. Many game developers routinely produce their own in-game currencies and create digital assets without necessarily facing, or recognizing that they may face, the same regulatory oversight and onerous KYC requirements that apply to other payment processors.[6]

Recently, the *EU's Fifth Anti-Money Laundering Directive* introduced AML obligations for cryptocurrency exchanges operating within member states which had to be complied with by 2020. This suggests significant changes are likely in the area of virtual currency regulation and this will inevitably prompt the industry to adopt new monitoring and compliance tools.

## 3 Advances in FinTech Necessitate a Parallel Increase in RegTech

FinTech refers to technology that aims to compete with traditional financial methods in the delivery of financial services, with challenger banks and virtual currency exchanges being prime examples.

With FinTech in a phase of rapid growth, it presents fresh challenges for regulators world-wide and highlights the need for parallel developments in regulatory technology to drive AML enforcement. Regulatory technology, also known as RegTech, uses information technology to enhance a company's regulatory processes in monitoring, reporting, and compliance. Firms in both the U.K. and U.S. have often struggled to find solutions to keep up with increasing regulation and compliance demands, and RegTech has emerged as a support tool to help ease this burden.

RegTech solutions are aimed at making it easier and cheaper for financial institutions to comply with ever-changing regulations by streamlining labor-intensive and costly tasks. With a United Nations estimate of $800 million to $2 trillion in money laundering annually, the global market for automated AML monitoring software is likely to continue to show strong growth.[7]

## 4 Advances in FinTech Necessitate a Parallel Increase in RegTech

Social media platforms have created yet another new environment for money laundering and pose a variety of emerging risks for financial institutions. The use of social media has evolved from simply connecting with friends to generating income for users who have learned to leverage the various platforms for personal gain.

Social media channels are filled with individuals hoping to find easy targets to swindle a few (or thousands of) dollars off, and the companies that run these apps are increasingly having trouble keeping up with perpetrators. Recently, a 22-year-old Instagram and YouTube social media influencer from New Jersey used her followers to unwittingly assist her in money laundering by convincing them to allow her to deposit stolen money orders into their accounts.[8]

Interestingly, on the other end of the scale, social media sites such as Facebook and LinkedIn can also be utilized as valuable AML investigative tools. These platforms can aid in identifying and evaluating individuals and businesses, determining links and networks between parties, and uncovering criminal connections. Leveraging social media as a resource tool can greatly enhance AML/CTF investigations.

**Ongoing developments in both technology and media will continue to be driving factors in the AML/CTF policy and enforcement agenda worldwide. To help safeguard your organization:**

- AML Compliance teams should be properly up to date on developments in the FinTech space and communicate emerging risks to management;
- Client risk profiles may need to change as a result of active use of novel FinTech offerings; and
- RegTech offerings should be regularly revisited to see whether improvements can be adopted for current AML programs.

We expect the AML/CTF landscape to look very different again in a few years from now and taking a proactive approach is critical to mitigate the associated risks, ensuring risk assessments, controls and processes remain appropriate and effective.

## About the Author

*Emilia Drozda, a Senior Manager with StoneTurn, is an experienced forensic accountant and investigator. In particular, she focuses on complex corporate dispute resolution, financial investigations and compliance monitoring.*

1 https://www.finextra.com/blogposting/16039/assessing-the-impact-of-global-aml-amp-sanctions-fines and https://www.businessinsider.com/financial-institutions-hit-with-regulatory-fines-since-2008-2020-1

2 https://www.bbc.com/news/technology-47751945

3 https://www.riskscreen.com/kyc360/news/nikolay-storonskys-revolut-freezes-accounts-in-money-laundering-bungle/

4 https://venturebeat.com/2019/07/20/crypto-can-prevent-money-laundering-better-than-traditional-finance/

5 https://www.businesswire.com/news/home/20181010005694/en/Ninety-Seven-Percent-97-Criminal-Bitcoin-Flows-Unregulated

6 https://www.acamstoday.org/online-video-games-regulatory-overview/

7 https://www.unodc.org/unodc/en/money-laundering/globalization.html

8 https://www.justice.gov/usao-nj/pr/ten-people-charged-15-million-fraud-scheme