ACAMS® TODAY Europe

The Magazine for Career-Minded Professionals in the Anti-Money Laundering Field

MAY—JUNE 2019 | VOL. 1 NO. 1

FINTECH: FRIEND or FOE to anti-financial crime?

Also in this issue:

Emerging sanctions challenges for global counter-terrorism

www.ACAMS.org | www.ACAMSToday.org

A publication of the Association of Certified Anti-Money Laundering Specialists® (ACAMS®), Miami, FL, USA

Advanced Anti-Money Laundering Certification

The next step in your professional career advancement

A step above the CAMS certification, our highly-regarded CAMS-Audit Advanced certification will develop your AML expertise and teach you the skills necessary to take on high-level audit responsibilities in any organisation.

Join the next cohort of CAMS-Audit graduates. Study in Amsterdam between 1 - 4 December 2019.

CAMS AUDIT


NICE
ACTIMIZE
Are you doing enough to stop illicit trafficking, organised crime and terrorism?
Autonomous Financial Crime Management
• AI-enabled financial crime & compliance platform
• Detect unusual behaviour earlier and faster
• Operationalise and automate the end-to-end process
• Financial crime experts
Visit NICE Actimize stand #16 to find out how to power your financial crime program
info@niceactimize.com
https://info.nice.com/Autonomus-AML.html

ACAMS TODAY Europe

The Magazine for Career-Minded Professionals in the Anti-Money Laundering Field

The award-winning *ACAMS Today* magazine is designed to provide accurate and authoritative information concerning international money laundering controls and related subjects. In publishing this work, neither the authors nor the association are engaged in rendering legal or other professional services. The services of a competent professional should be sought if such assistance is required. *ACAMS Today* is published four times a year for ACAMS members.

TO JOIN, contact:
ACAMS
Brickell City Tower
80 Southwest 8th Street,
Suite 2300
Miami, FL 33130

Tel. 1-305-373-0020
Fax 1-305-373-7788
Email: info@acams.org

Websites:
www.ACAMS.org
www.ACAMSToday.org

Twitter: @acamstoday

To advertise, contact:
Andrea Winter
Tel. 1-305-373-0020 ext. 3030
Email: awinter@acams.org

ACAMS

Follow the acclaimed *ACAMS Today* on Twitter, winner of the following awards:

HERMES AWARD

Platinum Award: Print Media, Writing, Publication Article: *De-Risking and the Effects on the World's Neediest*

Platinum Award: Print Media, Publications, Print Magazine, *ACAMS Today* June-August 2018

Platinum Award: Print Media, Writing, Publication Overall, *ACAMS Today* September-November 2018

AZBEE AWARDS

Regional Gold Award: All Content, Q&A, Southeast, *Lydia Cacho: The Defender of Human Rights*

Regional Silver Award: Design, Front Cover, Special Issue or Supplement, Southeast, *ACAMS Today* September-November 2018

Regional Silver Award: All Content, Q&A, Southeast, *Terry Forliti: Empowering Human Trafficking Survivors*

ADDY AWARDS

Best in Show for Publications

Gold Award: Collateral Material, Magazine Design, *ACAMS Today* September-November 2018

Gold Award: Collateral Material, Magazine Design, *ACAMS Today* June-August 2018

MARCOM AWARDS

Platinum Award: *ACAMS Today* June-August 2018 Table of Contents

Platinum Award: *Lawyers, Drugs and Money: AML in Popular Media*

Platinum Award: *ACAMS Today* Career Guidance Column

@acamstoday

rdc
Smarter Screening

Optimise your customer screening process with precise risk information and cutting-edge technology

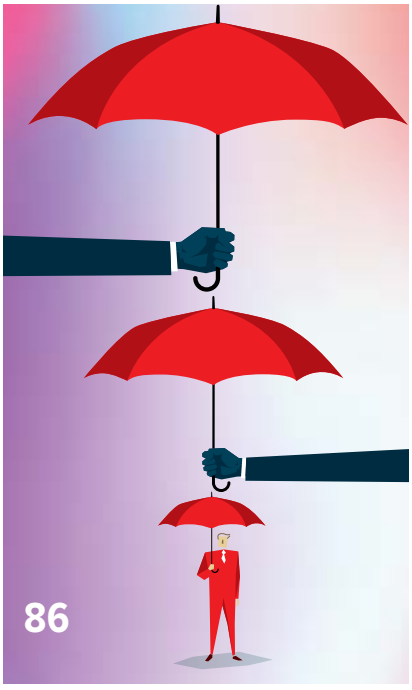
- Uncover hidden risk with integrated PEP, sanctions and adverse media intelligence
- Increase efficiency with configurable risk filters
- Automate onboarding decisions with sophisticated artificial intelligence

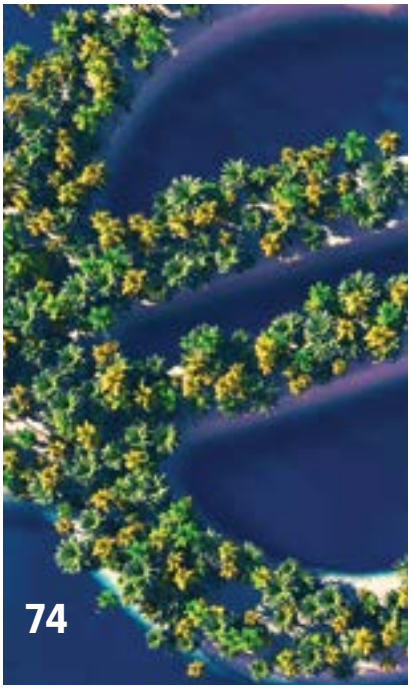
Find out more at **www.rdc.com**

Contents

ON THE COVER:

DEUTSCHE





FRANÇAIS

Renaissance

At 19 years old, I set out on an adventure and lifelong dream—to see Europe. Armed with my backpack and everything I thought necessary to survive a six-week excursion to the continent, I began visiting country-after-country. I learned from this thrilling adventure that Europe was more than what I had imagined and studied in college. This continent opened my eyes to different cultures, food, architecture, art and natural beauties that in my opinion should be experienced firsthand. It was my personal renaissance—it led to more trips and a longer stay in one of the most beautiful regions in the world.

ACAMS Today is having a renaissance of its own. I am proud to unveil the inaugural edition of *ACAMS Today Europe*. In addition to its cultural wonders, Europe is also one of the leaders in the fight against financial crime: From the European Union Directives, the General Data Protection Regulation and sanctions, to its continued fight against terrorist financing and more.

The lead article in *ACAMS Today Europe* poses the question, *Fintech: Friend or foe to anti-financial crime?* Seen as complementary to traditional bank accounts, digital bank accounts and e-wallet services are often regarded as lacking a culture of compliance. Learn possible solutions on how to tackle the risk of fintech banking.

The next featured article, *Emerging sanctions challenges for global counter-terrorism,* covers the latest changes in global sanctions and addresses the challenges that the transformation of the Islamic State has caused in combatting financial crime.

Also in this issue, an article on the notable changes to the Fifth AML Directive, and another on using suspicious activity report analysis to report the link between financial crime and gambling.

The inaugural *ACAMS Today Europe* edition contains articles not only in English, but also in German and French.

I would be remiss if I did not thank the newly formed *ACAMS Today* editorial committee—Europe for their invaluable contributions in both content and language expertise.

I hope *ACAMS Today Europe* will provide a renaissance of sorts to those of you continuously fighting financial crime. I am looking forward to meeting and speaking with many of you in Berlin this coming June.

See you soon, À bientôt, Bis bald,

Karla Monterrosa-Yancey, CAMS
editor-in-chief
Follow us on Twitter: @acamstoday

BERLIN
RISK

At BERLIN RISK we put **INTEGRITY** at the center of our services

BERLIN RISK is a risk and compliance advisory firm with a long-standing track record. We support private and public sector clients globally with:

- Investigations
- Integrity Due Diligence
- Reputational Risk Assessment
- Anti-Financial Crime Advisory Services

Insight. Integrity. Advantage.

www.berlinrisk.com

Annika Brunned, CAMS
Stockholm, Sweden

Annika Brunned is a compliance officer at Handelsbanken and head of the compliance international department covering Handelsbanken branches in Germany, Luxembourg, the Baltics, Poland, Singapore, Hong Kong, China and the United States. Brunned is an anti-money laundering (AML) compliance and financial crime prevention professional with over 30 years of practical experience within business, IT development and compliance at Handelsbanken.

After graduation, she started her career in Handelsbanken in the mid-1980s. She held many different positions including branch manager, head of Basel II implementation, trader on the money market, head of IT development, chief financial officer of Handelsbanken UK and head of the regional bank in northern Sweden. She has also been a member of the Handelsbanken Group Executives. When given the position as head of AML, counter-terrorist financing (CTF) and international sanctions in 2015, she developed a passion and enthusiasm for AML and CTF. Later this led to a new position as head of financial crime compliance.

Brunned has been an Association of Certified Anti-Money Laundering Specialists (ACAMS) member since 2017 and the last ACAMS conference she attended was the *11th Annual AML & Financial Crime Conference—Asia Pacific.*

Katarina Cook, CAMS
London, UK

Katarina Cook works as head of compliance and money laundering reporting officer for Europe Arab Bank in London. With a degree in Russian and political science, the move into the financial industry may not have seemed like the obvious choice for Cook. However, since the day Cook joined ABN AMRO (London) as a know your customer analyst in 2005, her interest in financial crime prevention resulted in a diverse career including many post-graduate diplomas and certifications covering compliance and anti-money laundering.

Cook has worked with all aspects of financial crime prevention, from policy writing to investigations and from management information development to training. Although London is where she spent most of her working life, she also worked for The Royal Bank of Scotland in the Netherlands for three years as head of conduct and regulatory affairs covering Netherlands and the Nordic region.

Cook is CAMS certified and is currently joint vice-chair for the Association of Certified Anti-Money Laundering Specialists United Kingdom Chapter.

Audrey Milesi, CAMS
Neuheim, Switzerland

Audrey Milesi lived and worked in Austria, Germany and London before moving to Switzerland in 2007. She began her career as an external auditor before moving to transaction services/mergers and acquisitions in the Big Four and transitioning into the industry. She led global financial compliance at the agrochemical company Syngenta and then moved to eBay to lead financial compliance for Europe/rest of the world.

Since joining the Association of Certified Anti-Money Laundering Specialists (ACAMS), Milesi has been an active advocate of the association in Switzerland. She is a founding member and chair of the newly launched Switzerland Chapter.

In 2017, Milesi started her own consultancy, A.M.C. Milesi—Flying CFO®, specializing in regulatory audits, anti-money laundering (AML), internal controls and compliance assistance to asset and fund managers as well as banks. She is also a regular speaker at conferences and has published articles about compliance and fraud matters.

As an ACAMS approved trainer, Milesi provides face-to-face as well as webinar-based trainings in English, German and French on AML, know your customer and anti-bribery and corruption topics.

Milesi holds a master's degree in commerce and international affairs as well as a master's in German. She is a Certified Anti-Money Laundering Specialist, Chartered Certified Accountant and Certified Fraud Examiner.

Sandijs Vectēvs, CAMS
Riga, Latvia

After 15 years in the financial sector, Sandijs Vectēvs returned to law enforcement in the area of financial intelligence. Prior to managing the analytical compartment of the Latvian financial intelligence unit, Vectēvs gained professional experience in various fields.

Vectēvs started his professional career more than 25 years ago in the police department as a detective in a homicide investigation squad. After many years in the police force, he took on a new challenge and decided to test his strength in the private sector in the field of anti-money laundering. The investigation of murders and money laundering is not the same, but the experience Vectēvs gained in murder investigations has served his entire future career. He carried over the following skillset from the public sector to the private sector of maintaining focus during difficult situations, keeping calm during a crisis and the perseverance to carry out his duties, which allows him to make the right decisions in a split second.

In the banking sector, Vectēvs has devoted 15 years to catching criminals and revealing their criminal financial flows. He plans to use this invaluable experience in the field of financial intelligence in the future. Latvia has declared an uncompromising fight on money laundering and Vectēvs has the honor of being part of this important fight for his country.

Annalise Vineer, CAMS
London, UK

Annalise Vineer commenced her career in insurance, dealing with fraud and contentious claims. Due to the complexity and litigious nature of her work, she undertook an advanced diploma in insurance to enhance her professional qualifications, knowledge and credibility. Vineer advanced her studies in this field and became a fellow of the Chartered Insurance Institute and a Chartered Insurance Practitioner.

Vineer then embarked on a master of science in forensic accounting, which enabled her to transition smoothly into anti-money laundering (AML) investigations in banking. She then moved to the Financial Conduct Authority where she worked in supervision, overseeing the behaviour and practices of a portfolio of firms. Having completed her M.S., Vineer transitioned back into banking and joined her current employer HSBC as manager of the European AML risk models. At the same time, she started a professional doctorate in criminal justice.

She then became the regional head of strategic analysis for HSBC's financial intelligence unit and was recently employed as senior risk quality assurance manager within the business financial crime risk team at HSBC. In 2018, Vineer completed her Certified Anti-Money Laundering Specialist certification and passed her professional doctorate with a thesis titled, "The Awkward Question: An Examination of Questioning Techniques Used by Banks to Prevent Financial Crime."

Catch the bad guys, avoid a penalty:

Can compliance have it all?

Welcome to the first issue of ACAMS Today Europe. ACAMS Today launched in 2002 as a membership benefit of a newly formed United States-based association of anti-money laundering (AML) professionals.

Today, the Association of Certified Anti-Money Laundering Specialists (ACAMS) is a global association of 73,000 members, and counting.

Like its award-winning parent *ACAMS Today,* the multilingual *ACAMS Today Europe* is helmed by Karla Monterrosa-Yancey and her fabulous team. We hope *ACAMS Today Europe* meets the needs of our ever-expanding European membership, which we are counting on for feedback and editorial contributions.

Karla's constant hand at *ACAMS Today* over the last 13 years reminds us that while much has changed for anti-financial crime (AFC) professionals, some things are timeless.

At our conference in Hollywood, Florida this April, speakers on a panel detailing lessons from major enforcement actions agreed that there are two bedrock priorities for AFC professionals: preventing and deterring crime; and achieving technical compliance with regulatory program requirements.

The two should be complementary, but the four panelists—who collectively represent decades of global compliance experience—agreed that at best they were in tension with one another and sometimes a Hobson's choice: tick the box to please the regulators or try to catch bad guys.

"I can think of the banks we used to supervise that got big fines, cease and desist orders, some of the biggest banks in the world," said Dan Stipano, former deputy chief counsel for the Office of the Comptroller of the Currency. "They would come and tell us, and their lawyers would say, 'yeah but we worked with the Manhattan District Attorney's Office.... We were instrumental in this criminal case.'"

"The response from examiners was 'that's great, but your CIP wasn't any good, and your KYC wasn't any good, and your transaction monitoring was weak,'" recounted Stipano, now a partner at Buckley LLP.

An audience question suggested that if you met the regulatory requirements, you would also catch criminals.

But no one on the panel let go of the potential for the two goals to diverge.

Praising the industry's cooperation with law enforcement, Rick McDonell, ACAMS executive director and a former Financial Action Task Force executive secretary, held up the example of the United Kingdom's Joint Money Laundering Intelligence Taskforce (JMLIT).

The initiative brings law enforcement and compliance professionals together to review files of ongoing investigations and is such a success that nine or 10 other jurisdictions have rolled out or plan to create similar bodies.

Markus Schulz, global head financial crime controls at Standard Chartered, said that JMLIT—and efforts like it—literally give meaning to AFC professionals' lives, connecting AML transaction monitoring and other forensic practices to catching criminals who destroy innocent lives.

Still, financial institutions do not get any extra credit for their commitment to work with law enforcement and they give up staff that might be dedicated to meeting regulatory demands, he said.

None of this is to give too much weight to some protests from the industry that the onerous penalties meted out over the past decade are about technical violations of regulation. Most of the hundreds of millions in penalties were levied for egregious behaviour.

Nor can the latest scandals involving Nordic and Baltic banks be said to involve minor errors, McDonell pointed out.

A small branch in Estonia funnelled $230 billion (US dollars) into the global financial system over several years through Danske Bank—at one point accounting for 10 percent of Danske's revenue.

That is a major red flag, Schulz quipped, adding with some humility, "I can only assume that some of that money is sitting in one or more of our banks," just not hundreds of billions.

After all, something is wrong when you cannot account for $1 billion (US dollars) going through your bank, Karim Rajwani, SVP, chief administrative officer at Scotiabank, seconded.

Knowing when $1 billion (US dollars)—or even smaller sums—goes through your institution, where it goes, and to whom depends on having in place policies and procedures mandated by regulation.

Fulfilling know your customer and transaction monitoring duties can, in this example, help you be a crime fighter and keep your regulator happy.

But as long as banks are given heavy to-do lists for compliance and multiple matters requiring attention from regulators they are likely to grumble, sometimes fairly and sometimes unfairly, that they are being burdened with too many niggling rules.

As we launch *ACAMS Today Europe* to serve the needs of a growing organization, we are aware that the tension over AFC priorities is unlikely to ever be resolved, but it is an important part of our mission to help our members at financial institutions, in the regulatory community and law enforcement to navigate through it. A

Kieran Beer, CAMS
director of editorial content
kbeer@acams.org
Follow me on Twitter: @KieranBeer

Emerging sanctions challenges for global counter-terrorism

With the attack on the village of Baghouz near the border between Syria and Iraq, Islamic State (IS)[1] is about to lose the last territorial stronghold in the Middle East.[2] This will end the recent tragic history of control over territory in the region from this terrorist organisation. However, this only concludes a first phase in the fight against IS and not the end of the organisation. The group has reacted to its continuous military defeats since 2016 by reorganising and transforming itself from a hierarchically organised group, focused on conquering and holding territory, into a loose covert network of terror cells—similar to that of al-Qaida—with a flat hierarchy that is focused on terror attacks.[3] Currently, this transformation is more advanced in Iraq than in Syria.[4] In the long term, the strategic question remains on whether the two global terror networks IS and al-Qaida are going to converge into one or remain as two separate terror organisations.

This structural transformation also affects the way IS raises and spends money. With the loss of territorial control, IS also relinquished its ability to generate funds from the systematic exploitation of natural resources and looting of antiquities and "taxing" of the local population. However, by not having to administer large cities and infrastructure, the group's expenditure has reduced significantly. Furthermore, the group maintains access to funds it had removed from Iraq and Syria since 2014 through money couriers and informal payment channels.[5] Estimates of funds available to IS range between $50 million to $300 million (US dollars).[6]

Acting as a covert network that tries to inspire attacks of individuals and cells within the region and beyond will likely mean that financial flows to and from the IS core in Iraq and Syria are going to be based on transactions of small sums via informal payment channels or money couriers. This is a challenge to efforts in combatting terrorist financing. Furthermore, it is expected that individual IS cells in the region and beyond will self-finance their activities, further reducing the need for international financial flows within the group.[7] However, due to the significant size of funds under control of the group, IS has to find ways to manage these funds as well as generate finances within the conflict zone. The global counter-terrorism sanctions regime of the United Nations Security Council (UNSC) is an effective instrument to counter these threats.

Changes in the global sanctions regime to respond to the challenge by IS

In response to the al-Qaida terror attacks in Nairobi and Darussalam in 1998, the UNSC established a global sanctions regime, targeting the al-Qaida network and the Taliban regime in Afghanistan with Resolution 1267 (1999).[8] UNSC continuously updates this sanctions regime to respond to the changing threat environment. In response to the emergence of IS, UNSC—in cooperation with the sanctions committee and the IS, and Taliban Monitoring Team—made significant adjustments to the global sanctions' architecture. Since 2014, these changes aim to provide better, more precise information to member states of the United Nations (U.N.) as well as private sector sanctions implementers to target the financial activities of IS more specifically and to counter the new threat posed by foreign terrorist fighters (FTFs), returnees and relocating FTFs.

With Resolutions 2178 (2014)[9] and 2368 (2017),[10] UNSC addressed the issue of FTFs, returnees and relocators. In these resolutions, UNSC asked member states to criminalise the travel of individuals to join IS and collect information via

the Advanced Passenger Information and passenger name record of international airlines to identify FTFs, returnees and relocators. This allowed governments to identify, monitor and intercept travelling terrorists more broadly. With Resolutions 2199 (2015),[11] 2214 (2015)[12] and 2253 (2015),[13] UNSC specifically targeted the activities of IS in Iraq, Syria as well as Libya, and the emerging global network of the organisation. These resolutions not only added IS and its global leadership to the already existing sanctions list but also introduced important new aspects to the sanctions regime, such as the exploitation of natural resources like oil and the looting of antiquities by IS. UNSC also passed a range of resolutions addressing specific forms of criminal behaviour employed as IS-funding activities. Resolution 2347 (2017)[14] addressed the ability of IS to generate funds through the looting, smuggling and sale of cultural artefacts and established a range of measures enabling both member states and private sector stakeholders to defend against the misuse of the international antiquities market for terrorism financing.[15] Finally, Resolutions 2331 (2016)[16] and 2388 (2017)[17] target the attempts by IS to obtain funds through involvement in human trafficking.

In addition to these legal adjustments, UNSC also decided to technically update the "ISIL (Da'esh) & Al-Qaida Sanctions List" to make it more compatible with current technical standards of compliance software.[18] This technical update was accompanied by the introduction of hyperlinks in the identification data fields of the sanctions list that connects the entries of the respective individuals and entities to the public version of the INTERPOL UNSC Special Notices issued for them.[19] These special notices include pictures and fingerprints of sanctioned individuals, enabling implementers to also use biometric data for matching purposes. Finally, UNSC asked the secretary general to regularly and publicly report on the changing threat posed by IS, in addition to the public reports by the IS, al-Qaida and Taliban Monitoring Team.[20] These reports outline the main developments in terrorist tactics employed by IS—including changing trends in IS financing—and can be used for the development of typologies.

Emerging challenges for combatting the financing of IS

The current transformation of IS financing is presenting four major challenges for those combatting its illicit finance activities: the misuse of illicit IS investments, the misuse and extortion of the charitable sector, informal payment channels and cryptocurrencies.

In several instances, IS seemed to have laundered sums it had illegally obtained and reinvested them in newly established companies in the region; for example, in the agricultural, real estate and money exchange offices.[21] The involvement of IS in parts of the licit economy in the region potentially requires enhanced due diligence and know your customer procedures. This will likely become a significant challenge during the ongoing reconstruction activities in Iraq and potential reconstruction in Syria.

This is connected to the threat of an increase in the misuse of the charitable sector by IS, not only to transfer funds but also through the extortion of local implementation partners of humanitarian aid programmes. This is not a new challenge. In the past, al-Qaida regularly misused charitable organisations for its activities.[22] However, since IS is no longer able to obtain finances through a large-scale exploitation of natural resources or "taxation" of local populations under its control, extorting charitable organisations and companies involved in reconstruction is likely to increase significantly.

The role of informal payment channels in terrorist financing is a well-documented challenge.[23] However, the challenges of financial inclusion encountered in conflict areas, such as Iraq, and the difficulties in transferring funds to Syria—due to international sanctions against the Syrian financial sector—create an increased risk of bulk cash transfers and informal payment mechanisms being misused by IS hiding its finance, activities and transfer of funds.

Finally, a newly emerging challenge is the misuse of cryptocurrencies by IS. Already for a number of years, IS members have demonstrated an interest in this new technology.[24] So far, the exchange of cryptocurrencies in fiat money in conflict areas presents a difficulty for IS and has limited IS' ability to use cryptocurrencies to raise money or transfer funds.[25] However, cryptocurrencies have a global nature and are becoming more accessible. On top of that, there is the enhanced ability to anonymise the identity of users in combination with the fact that in many member states, regulation of this technology is missing or only currently emerging. This offers IS an opportunity to misuse this technology to store funds it has already obtained. The Counter Extremism Project is currently developing a range of regulatory recommendations in this regard.

Due to these challenges, effectively combatting the financing of terrorism will continue to depend on a variety of methods. Some of these are the continued adjustment of typologies, information on the identities of terrorist financers and facilitators, the mapping of financial flows and the effective regulation of new technologies to ensure a sufficient level of transparency. In all these aspects, the global counter-terrorism sanctions regime of UNSC will continue to play a crucial role, not only for agencies charged with developing countermeasures of member states, but for implementers in the private sector. Knowledge of the information provided by the sanctions regime and the development and strengthening of effective public-private partnerships within member states are central elements in combatting IS' evolving financial activities.

Dr. Hans-Jakob Schindler, senior director, Counter Extremism Project, New York, NY, USA and Berlin, Germany and former coordinator ISIL, Al-Qaida and Taliban monitoring team, United Nations Security Council, hjschindler@counterextremism.com

[1] Included under reference number QDe.115 "Al-Qaida in Iraq" as AKA p) "Islamic State in Iraq and the Levant" (ISIL) by the United Nations Security Council in its global ISIL (Da'esh) & Al-Qaida Sanctions List.

[2] Ben Wedeman and Jay Croft, "Heavy fighting reported as US-backed forces attack last ISIS stronghold in Syria," CNN, 11 March 2019, https://www.cnn.com/2019/03/10/middleeast/syria-isis-stronghold-sdf/index.html

[3] "Third report of the Secretary-General on the threat posed by ISIL (Da'eash) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat," United Nations Security Council, 30 September 2016, http://undocs.org/S/2016/830

[4] "Letter dated 15 January 2019 from the Chair of the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'eash), Al-Qaida and associated individuals, groups, undertakings and entities address to the President of the Security Council," United Nations Security Council, 15 January 2019, http://undocs.org/S/2019/50

[5] Howard J. Shatz, "To Defeat the Islamic State, Follow the Money," RAND Corporation, 10 September 2014, https://www.rand.org/blog/2014/09/to-defeat-the-islamic-state-follow-the-money.html

[6] "Letter dated 15 January 2019 from the Chair of the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'eash), Al-Qaida and associated individuals, groups, undertakings and entities address to the President of the Security Council," United Nations Security Council, 15 January 2019, http://undocs.org/S/2019/50

[7] "Eighth Report of the Secretary General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat," United Nations Security Council, 1 February 2019, para. 14, http://undocs.org/en/S/2019/103

[8] "Security Council pursuant to resolutions 1267 (1999) 1989 (2011) and 2253 (2015) concerning ISL (Da'esh) Al-Qaida and associated individuals groups undertakings and entities)," United Nations Security Council, https://www.un.org/securitycouncil/sanctions/1267

[9] "Resolution 2178 (2014)," United Nations Security Council, 24 September 2014, http://unscr.com/en/resolutions/doc/2178

[10] "Resolution 2368 (2017)," United Nations Security Council, 20 July 2017, http://unscr.com/en/resolutions/doc/2368

[11] "Resolution 2199 (2015)," United Nations Security Council, 12 February 2015, http://unscr.com/en/resolutions/doc/2199

[12] "Resolution 2214 (2015)," United Nations Security Council, 27 March 2015, http://unscr.com/en/resolutions/doc/2214

[13] "Resolution 2253 (2015)," United Nations Security Council, 17 December 2015, http://unscr.com/en/resolutions/doc/2253

[14] "Resolution 2357 (2017)," United Nations Security Council, 24 March 2017, http://unscr.com/en/resolutions/doc/2347

[15] Ibid. See in particular par. 17.

[16] "Resolution 2331 (2016)," United Nations Security Council, 20 December 2016, http://unscr.com/en/resolutions/doc/2331

[17] "Resolution 2388 (2017)," United Nations Security Council, http://unscr.com/en/resolutions/doc/2388

[18] "Resolution 2253 (2015)," United Nations Security Council, 17 December 2015, http://unscr.com/en/resolutions/doc/2253. See par. 48.

[19] "Sanctions List Materials," United Nations Security Council, https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list. Each list entry is accompanied by a narrative summary for reasons of listing that includes additional biographical information. These narrative summaries are available from "Narratives Summaries of Reasons for Listing," United Nations Security Council, https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list/summaries. The INTERPOL-United Nations Security Council Special Notices for individuals are available from "View UN Notices—Individuals," INTERPOL, https://www.interpol.int/en/How-we-work/Notices/View-UN-Notices-Individuals. The notices for entities are available from "View UN Notices - Entities," INTERPOL, https://www.interpol.int/en/How-we-work/Notices/View-UN-Notices-Entities

[20] "Resolution 2253 (2015)," United Nations Security Council, 17 December 2015, http://unscr.com/en/resolutions/doc/2253; "Resolution 2368 (2017)," United Nations Security Council, 20 July 2017, http://unscr.com/en/resolutions/doc/2368

[21] "Letter dated 17 January 2018 from the Chair of the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011), and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'aesh), Al-Qaida and associated individuals, groups, undertakings and entities addressed to the President of the Security Council," United Nations Security Council, 26 January 2018, https://undocs.org/S/2018/14

[22] "Wafa Humanitarian Organisation" United Nations Security C ouncil, https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list/summaries/entity/wafa-humanitarian-organisation

[23] "Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)," Financial Action Task Force, February 2015, http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-IS.pdf; and "Emerging Terrorist Financing Risks," Financial Action Task Force, October 2015, http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf

[24] Ankit Panda, "Cryptocurrencies and National Security," Council on Foreign Relations, 28 February 2018, https://www.cfr.org/backgrounder/cryptocurrencies-and-national-security

[25] Yahya Fanusie, "Survey of Terrorist Groups and Their Means of Financing," House Financial Services Committee Subcomittee on Terrorism and Illicit Finance, 7 September 2018, https://www.fdd.org/wp-content/uploads/2018/10/09-07-18-Yaya-Fanusie-Written-Testimony.pdf

A smorgasbord of regulations

Blockchain technology offers a wide array of solutions that challenge traditional business models but this innovation needs updated governance policies to balance efficiency and public safety. Blockchain technology can allow for autonomous users to transfer wealth quickly, worldwide, at any time and without any middlemen using its heretofore most successful use case—virtual currencies. This technology increases transparency and traceability because typically all blockchain transactions are recorded in a distributed ledger; however, this technology is not immune to risks associated with market abuse, money laundering and terrorist financing.

Regulators worldwide have recognised the emerging risks related to virtual currencies and have taken different approaches to mitigate and manage these risks. The method of some regulators has been to define virtual currencies and virtual currency service providers under existing regulatory frameworks like traditional financial service providers, thereby subjecting them to similar anti-money laundering/counter-terrorist financing (AML/CTF) requirements. Other regulators have acknowledged the importance of providing regulatory frameworks specific to virtual currencies and have created safe spaces to grow this burgeoning industry.

Today, the industry remains largely unregulated in many jurisdictions and guidelines for those jurisdictions that are regulated lack uniformity. In fact, according to a report published by CipherTrace in October 2018, "97% of criminal Bitcoin directly received by exchanges flowed into those located in countries with weak AML laws" and "4.7% of Bitcoin received by exchanges in countries with weak regulation is criminal."[1] These statistics are based on confirmed cases of bitcoin transfers from criminals, and it demonstrates criminals' propensity to exploit countries with weak anti-money laundering (AML) laws. For this reason, it is imperative to set a global standard for a regulatory framework that addresses the emerging opportunities and risks presented by virtual currencies and virtual currency service providers. This article will provide a brief introduction to the regulatory framework proposed by the United States (U.S.), European Union (EU), Switzerland, United Kingdom (U.K.), Japan, Malta and the Financial Action Task Force (FATF). In addition, the risks associated with unregulated markets and the international nature of these risks will be examined through the alleged money laundering case of Alexander Vinnik.

United States

The United States (U.S.) can be considered the first country to have implemented regulations on virtual currencies. In March 2013, the Financial Crimes Enforcement Network (FinCEN) issued guidance that defined exchangers and administrators of virtual currencies as money transmitters, a type of money services business (MSB) under the Bank Secrecy Act of 1970 (BSA).[2] Any entity the BSA defines as an MSB must establish and maintain an effective AML program. Effectively, this definition puts major U.S. nexuses for virtual currencies in a position to combat money laundering and terrorist financing. This decision was an important change in the history of virtual currencies because it provided the world with a clear sign that innovative instruments used to transfer wealth, such as virtual currencies, must be regulated to control the risks of nefarious actors using them. It also showed that the instrument itself did not have to be defined as a currency, commodity or security; in order to be regulated. Instead of focusing on definitions, these regulations highlighted the importance of the risks posed by entities that use these instruments, and the controls that could be affected using existing laws.

Among other requirements, operating under the BSA and within the supervision of FinCEN requires exchangers and administrators to develop AML policies and procedures, file suspicious activity reports (SARs), respond to law enforcement requests and develop customer identification programs (CIPs). The information that regulated virtual currency MSBs gather through their CIP and SAR filings is invaluable to law enforcement and regulators. This is because transactions and deposit addresses on blockchains are displayed only as alphanumeric codes, which gives this activity perceived anonymity. In compliance with CIP requirements, MSBs verify a customer's identity and bank accounts, which can be linked to the customers' virtual currency deposit address(es), thereby bridging the gap in data between the traditional banking system and the virtual currency system.

In November 2018, the importance of matching identifiable information to virtual currency data (i.e., deposit addresses) was demonstrated by the Office of Foreign Assets Control (OFAC) when they provided the public with the identities and associated deposit addresses of two Iranian nationals that helped convert bitcoins received from a ransomware scheme into fiat.[3] Since these deposit addresses are traceable on the blockchain, virtual currency service providers can leverage this information to identify direct connections between their users and the individuals identified by OFAC.

Switzerland

Switzerland went a step further than the U.S. and introduced virtual currency companies to formal licensing structures and requirements, beyond those of an MSB. In October 2018, Switzerland's Financial Market Supervisory Authority (FINMA) awarded the world's first asset management licence to a virtual currency platform,[4] essentially giving this company the ability to operate like traditional asset managers in Switzerland. Virtual currency exchanges in Switzerland may seek asset management licences through FINMA. The Swiss Bankers Association (SBA) also issued guidelines that can help banks assess the risk of virtual currency service providers, including specific know your customer (KYC) and AML checks banks can conduct for Initial Coin Offerings (ICO)—business processes that involve funding and launching new tokens, similar to initial public offerings. The SBA's guidelines can help virtual currency providers gain access to traditional banking services.

FINMA also adopted a fintech licensing program effective January 1, 2019, which will allow non-bank institutions to accept public deposits up to 100 million Swiss francs and hold security tokens without obtaining additional securities dealer licensing. This licensing program is another way Swiss regulators have removed barriers to entry for virtual-currency-based businesses while taking measures to regulate the industry.

FINMA appears to take on a more conservative approach when considering liquidity, credit and market risk of virtual currencies from institutional investors' trading activities in virtual currencies. For example, it cites a trading cap for virtual currencies of 4 percent of total capital for institutional investors and suggests a risk weighting of 800 percent for virtual currencies at the high end due to credit risk, liquidity risk and the volatility of the market. There are currently no regulations specific to virtual currencies in Switzerland; however, virtual currency businesses are subject to current AML and securities regulations.

European Union

In June 2018, the Fifth AML Directive (5AMLD) included virtual currency exchange platforms and custodian wallet providers as obliged entities. This means that by January 2020, EU member states will require virtual-currency-centric obliged entities to implement AML/CTF controls. This also means that member states must have established laws, regulations and administrative provisions to accommodate the virtual currency industry.

The European Securities and Markets Authority (ESMA) along with the European Banking Authority (EBA) have also published reports on ICOs and virtual currencies. Both authorities have raised concerns over the applicability of current EU laws to virtual currencies. One conclusion both publications note is that current EU regulations do not govern most of the virtual currency activity. Therefore, regulatory responses at the national level are uncoordinated and seem to diverge.

Virtual currencies that qualify as financial instruments will be governed by the Markets in Financial Instruments Directive II (MiFID II). Interpretations of the MiFID II differ at the national level, and EU member nations have different interpretations of this directive. For example, there are different interpretations of whether MiFID II obligations apply at the fund level or fall to the management company. The MiFID II typically governs investment firms providing portfolio management services. However, in some EU countries, investment firms that provide collective portfolio management services and are governed by securities regulations are allowed to provide portfolio management services without being registered as an investment firm. The result is, again, misalignment among European states when it comes to regulating virtual currencies.

Current EU regulations do not govern most of the virtual currency activity

ICOs, security tokens and utility tokens can provide opportunities for innovation and efficiencies in the financial sector

For this reason, the ESMA and EBA reports advise that the European Commission set regulatory standards to create consistency in risk mitigation efforts.

According to a study conducted by Statis Group, 11 percent of ICO funding, or $1.34 billion (US dollars) out of $11.9 billion (US dollars), in various tokens went to scams in 2018.[5] Pincoin was a significant contributor, having been responsible for a $660 million (US dollars) ICO exit scam that victimised 32,000 investors. Issuing warnings to consumers regarding the risks associated with ICO investments does not appear to provide sufficient investor protection. ESMA Chairman Steven Maijoor acknowledged that the current lack of regulation of virtual currencies is leaving consumers exposed to substantial fraud risk through ICOs. On January 9, 2019, ESMA issued a report on ICOs and virtual currencies advising that specific virtual currencies that do not qualify as financial instruments or electronic money should be regulated by a set of rules tailored specifically to address their unique risks.

United Kingdom

The United Kingdom (U.K.) published the Sanctions and Anti-Money Laundering Act 2018, allowing the U.K. to establish its own AML/CTF regulations when it exits the EU. The U.K. is likely to adopt the 5AMLD as a minimum standard because the deadline set in the directive falls within the U.K.'s exit from the EU.

The Cryptoassets Taskforce launched in March 2018, consisting of the HM Treasury. The Financial Conduct Authority and the Bank of England recently published its final report, where it defines three different types of virtual currencies: exchange tokens, security tokens and utility tokens. Exchange tokens that utilise blockchain are not issued or backed by a central body and are used as a means of exchange (e.g., bitcoin). Security tokens are specified investments, transferable securities or financial instruments that provide rights such as ownership, repayment or entitlement to a share in future profits. Finally, utility tokens can be redeemed for access to a specific product or service and typically utilise a blockchain platform.

The report makes it clear that virtual currencies did not fit the criteria of traditional currency. Therefore, ICOs, security tokens and utility tokens can provide opportunities for innovation and efficiencies in the financial sector. Finally, the report proposes prohibitions on the sale of all exchange token derivatives to retail consumers. Excluded from this proposal are derivatives on virtual currencies that qualify as securities, although they could be subject to restrictions from other security authorities such as ESMA.

Financial Action Task Force

In June 2015, FATF released guidance on applying a risk-based approach when mitigating money laundering/terrorist financing risks related to virtual currencies. The purpose of FATF's guidance was to instruct centralised and decentralised providers of virtual currency payment products and services (VCPPS) on how to apply a risk-based approach to AML/CTF processes, and how to implement applicable FATF Recommendations.[6]

In October 2018, FATF made an official amendment to Recommendation 15—New Technologies. Initially, Recommendation 15 focused on mitigating the risk that could arise from the development and application of new technologies. The October 2018 amendment was specific to virtual currencies and focused on requiring countries to establish AML/CTF regulations for virtual asset service providers (VASP), which includes exchanges, certain types of wallet service providers and providers of financial services for ICOs.[7] In addition, VASPs would need to be licenced and registered with the appropriate regulatory body to operate. Important implications for a jurisdiction's regulator include, but are not limited to, controlling the existence of VASPs (e.g., revoking licences, rejecting licence applications, preventing criminals from becoming beneficial owners of VASPs), monitoring VASPs' AML/CTF compliance and taking punitive measures for non-compliance.

FATF set June 2019 as the final adoption date for the prescribed regulatory requirements concerning virtual currencies. The FATF's 40 Recommendations to combatting money laundering and terrorist financing are considered the global standard. This amendment is essential in creating a consistent approach toward AML/CTF internationally for virtual currencies. Furthermore, countries that are not compliant with the amended Recommendation 15 or deficient in its implementation may become designated as high-risk and therefore subject to increased diligence requirements by FATF-compliant countries and barriers to obtaining vostro accounts with large international banks. Gaining guidance on the responsibilities of VASPs may help for setting standardised AML/CTF practices worldwide, but it is equally important that indicators of suspicion be communicated so that VASPs can consistently provide law enforcement with useful SARs. Given the importance of FATF standards in shaping jurisdictional regulations, consultation from the virtual currency industry, law enforcement, traditional banking and national regulators is indispensable for the creation of effective FATF Recommendations.

Japan

Japan has one of the largest virtual currency markets in the world and has been proactive in accepting and regulating virtual currency exchanges. It has also been home

to some of the biggest virtual currency thefts. Japan accounted for a significant portion of the $950 million (US dollars) worth of virtual currency that was stolen from exchanges in 2018.[8] Japan-based exchanges Coincheck and Zaif[9] saw losses of $530 million (US dollars) and $60 million (US dollars), respectively, in various tokens due to theft. In response to these attacks, the Financial Services Agency gave the virtual currency industry self-regulating status by establishing the Japanese Virtual Currency Exchange Association (JVCEA) as the self-regulatory body. The group is considering placing a cap on customer deposits that can be managed online on hot wallets (wallets where keys are held online) of 10-20 percent,[10] as funds placed in hot wallets can be a target for hackers. Security standards around custodial services such as these can go a long way toward protecting virtual currency consumers and improving the reputation of the virtual currency sector.

The JVCEA also issues business improvement orders that may involve financial penalties. Zaif has two improvement orders so far: one for the "[e]stablishment of an effective risk management system" and a second for the "[e]stablishment of a system to respond appropriately to customers." Another virtual currency exchange, Quoine, indicated that the order they received pertains to compliance, KYC and AML. The introduction of a watchdog that can monitor the level of security and AML controls of Japanese virtual currency exchanges as well as enforce the regulations acts as a preventative measure to mega-heists like the ones Japan saw in 2018.

Japan also requires that virtual currency exchanges report suspicious activities. Japanese law enforcement reported that the number of suspicious transaction reports from virtual currency exchanges increased tenfold after a bill came into effect in April 2017, which obliges virtual currency exchanges to report suspicious activity. Such regulations pave the way for virtual-currency-based businesses and law enforcement to work together to combat money laundering and terrorist financing. In 2018, virtual currency exchange ShapeShift reported that they assisted with 60 law enforcement inquiries from around the world, 43 of which came from countries with strong AML regulations such as Germany, the U.K., France, the U.S., Canada, Switzerland, Australia and the Netherlands.

Malta

Virtual currencies and blockchain technology offer great potential growth for the financial sector and beyond. Therefore, it is not surprising that countries worldwide are competing to attract players in this burgeoning sector to their doors. From amongst the virtual-currency-friendly nations, Malta has made an effort to stand out. Malta is recognised as the first country to create a regulatory framework dedicated to virtual currencies and blockchain technology. Typically, the focus of regulators has been to mitigate emerging risks associated with virtual currencies by including them in existing compliance frameworks for AML/CTF and financial securities. Malta's regulatory framework is unique from other regulatory frameworks because it includes policies that promote the development of blockchain technology. Three acts will govern the regulatory framework: The Virtual Financial Assets Act (VFAA), Malta Digital Innovation Authority Act (MDIA) and the Innovative Technology Arrangements and Services Act.[11]

The VFAA establishes compliance and licensing requirements for virtual currency financial service providers and regulates different aspects of ICOs, such as procedures on issuances and white paper registration. In addition, the VFAA prohibits market abuse on exchanges and establishes regulatory and investigative powers. The MDIA grants authority to the Malta Digital Innovation Authority to develop and enforce policies that promote the development and use of blockchain in a manner that is ethical and in line with regulatory requirements. The Innovative Technology Arrangements and Services Act provides the framework for the voluntary certification of innovative technology arrangements (e.g., software for distributed ledger technology, smart contracts, etc.).

Virtual currencies and blockchain technology offer great potential growth for the financial sector and beyond

The international money laundering risks of insufficient regulations

In July 2017, the U.S. Department of Justice (DOJ) indicted Alexander Vinnik for allegedly using the exchange BTC-e to launder proceeds of crimes, including bitcoin from the infamous Mt. Gox hack where 850,000 bitcoins were stolen from the exchange's users. In its address to the public, the DOJ stated, "[a]ccording to the indictment, since its inception, Vinnik and others developed a customer base for BTC-e that was heavily reliant on criminals, including by not requiring users to validate their identity, obscuring and anonymising transactions and source of funds, and by lacking any anti-money laundering processes."[12] Criminals allegedly used this infrastructure to operate and receive funds from cybercrimes such as virtual currency hacking (theft), ransomware schemes, identity theft and various fraud scams. Vinnik allegedly managed multiple BTC-e accounts as well as accounts at other exchanges to obscure the path of hacked bitcoin, such as the Mt. Gox hack, and it is possible that these other exchanges had weak AML controls, if any. It was reported that BTC-e received $4 billion (US dollars) worth of bitcoin, which demonstrates the scale and reach of this scheme.

Appropriately, a collaborative approach between nations was used to investigate and arrest Vinnik. According to FBI special agent Amy Hess, "the arrest of Alexander Vinnik is the result of a multi-national effort and displays the benefits of global cooperation among U.S. and international law enforcement."[13] The ease in transferring ill-gotten wealth using virtual currencies is a global issue. Therefore, nations need to collaborate in their effort to combat money

laundering. This effort will require a consistent approach to AML; otherwise, nations' efforts will remain siloed, and criminals will remain mobile.

The way forward

In the next two years, the regulatory landscape is expected to change significantly with the final adoption and enforcement of regulations guided by FATF's amendment in June of 2019 and the EU's 5AMLD directive in January 2020. To some, these regulations may seem like an impediment to the virtual currency industry's growth, but virtual currencies and the underlying blockchain technology that supports it will be poised to expand further if the industry and its participants can establish trust with governments, regulators, financial institutions and the general public. Trust can occur when global minimum standards combined with local laws, regulations and enforcement provisions, can create a system of accountability. Companies in the virtual currency space often have difficulties in acquiring and keeping banking relationships necessary for sustainable business growth and instances of operators with weak AML/CTF controls worsen this problem for companies with appropriate compliance programs. Consistent regulations that emphasise public safety without stifling the growth of business and technology can be beneficial for the virtual currency sector and the public at large. For this reason, efficient and pragmatic regulations that draw from the knowledge of responsible virtual currency operators and law enforcement can best handle the related money laundering/terrorist financing risks.

Regulators have taken measures to mitigate risks associated with virtual currencies by placing controls on the industry and its participants. While a consistent approach to global minimum standards is critical, it is also important that regulators tailor their framework to mitigate risks that are unique to virtual currencies. Forcing legacy standards from the traditional financial industry unto virtual currencies is not always warranted and doing so can stifle growth and may even lead to unnecessary reporting and the related privacy issues. In the case of virtual currency regulations, a cohesive starting point is necessary, but in the long run, a flexible and far-sighted approach that can change with technological innovations will likely work more efficiently than a one-size-fits-all approach. A

Julian Arriagada, CAMS, manager-compliance, Tether, Julian@tether.to

Yasmine Ibrahim, analyst-compliance, Tether, Yasmine@tetehr.to

Contributor: Leonardo Real, chief compliance officer, Tether, Leo@tether.to

The ease in transferring ill-gotten wealth using virtual currencies is a global issue

1 "Cryptocurrency Anti-Money Laundering Report 2018 Q3," CipherTrace, 2018, https://ciphertrace.com/crypto-aml-report-2018q3.pdf

2 "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," Financial Crimes Enforcement Network, 18 March 2013, https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf

3 "Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses," U.S. Department of the Treasury, 28 November 2018, https://home.treasury.gov/news/press-releases/sm556

4 Matthew Allen, "Crypto Fund wins first Swiss crypto asset management licence," *Swissinfo,* 9 October 2018, https://www.swissinfo.ch/eng/finma-breakthrough_crypto-fund-wins-first-swiss-crypto-asset-management-license/44461088

5 Ana Alexandre, "New Study Says 80 Percent of ICOs Conducted in 2017 Were Scams," *Cointelegraph,* 13 July 2018, https://cointelegraph.com/news/new-study-says-80-percent-of-icos-conducted-in-2017-were-scams

6 "Guidance for a Risk-Based Approach to Virtual Currencies," Financial Action Task Force, June 2015, http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html

7 "Outcomes FATF Plenary, 17-19 October 2018," Financial Action Task Force, 19 October 2018, http://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-plenary-october-2018.html

8 "Cryptocurrency Anti-Money Laundering Report 2018 Q4," CipherTrace, 2018, https://ciphertrace.com/wp-content/uploads/2019/01/crypto_aml_report_2018q4.pdf

9 "Cryptocurrency Anti-Money Laundering Report 2018 Q3," CipherTrace, 2018, https://ciphertrace.com/crypto-aml-report-2018q3.pdf

10 Erik Gibbs, "JVCEA to tighten crypto storage regulations," Squire Mining, https://squiremining.com/category/japan-virtual-currency-exchange-association/

11 "FinTech," Malta Financial Services Authority, https://www.mfsa.com.mt/fintech/

12 "Russian National and Bitcoin Exchange Charged In 21-Count Indictment For Operating Alleged International Money Laundering Scheme and Allegedly Laundering Funds From Hack Of Mt. Gox," The United States Attorney's Office Norther District of California, 26 July 2017, https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged

13 "Russian national and bitcoin exchange indicted in multi-billion dollar money laundering scheme," U.S. Immigration and Customs Enforcement, 26 July 2017, https://www.ice.gov/news/releases/russian-national-and-bitcoin-exchange-indicted-multi-billion-dollar-money-laundering

FINTECH: FRIEND or FOE

to anti-financial crime?

Author's note: The discussion of "fintechs" in this article will be referring to digital bank accounts (e.g., Monzo) and other e-wallets account services (e.g., Apple Pay).

Fintechs are digital bank accounts and e-wallet services. There are more and more digital players in the market offering payment accounts, money pots or remittances services. What is new is that end-user adoption is growing quickly too.[1] There is not a week without the media mentioning that challenger banks (aka "neo banks") like Monzo, Revolut or N26 are increasingly enrolling more and more customers.[2]

At the same time, the number of customers that traditional banking institutions are losing does not seem so alarming. So what is happening? Why is there no net transfer from traditional banks toward fintechs?

Some of the reasons cited by end users for adopting fintech accounts include the ease of use, competitive prices and better quality of service

Customers are adopting these new payment systems and platforms without leaving their traditional bank.[3]

Most can think of reasons depending on their own situations and behaviours as to why they should keep both a traditional bank account and a fintech account. Indeed, many of the people deciding to switch to fintech banking simply do not close their "traditional" bank accounts but rather maintain both for different reasons.For instance, users may need a way to fund their fintech accounts, thus making their traditional bank accounts just a way to funnel funds into their digital accounts, or their traditional bank proposes services that their fintech account providers do not yet provide, such as investment, loans, etc. Another reason could be if users do not yet completely trust their fintech account provider. In the European Union (EU), until a fintech account provider gets an actual banking licence, the funds deposited by their customers are not guaranteed through the EU deposit guarantee schemes,[4] which protect depositors' savings by guaranteeing deposits of up to €100,000.

On the other hand, some of the reasons cited by end users for adopting fintech accounts include the ease of use, competitive prices and better quality of service.[5]

But could the myriad of new alternatives that allow anyone to open a fintech account and be granted with payments (typically, a payment card) in a matter of minutes be facilitating financial crimes?

Raising awareness on the use of fintechs for possible financial crimes purposes

How many readers already have a fintech account? Anti-money laundering (AML) professionals may be curious about these (sometimes only supposedly) disruptive ways of conducting customer registration, ID collection and vertification, and in general know your customer (KYC) and may even have more than one fintech and/or challenger's account. But what information is being requested when registering for a new account?

Basically, the same information amongst the different providers: personal data supported by a government-issued ID and sometimes a national tax ID supported by nothing.

One can virtually open as many accounts as there are fintech providers able to do so (essentially providing you with an international bank account number).

What is the difference between regular or more traditional banks, financial institutions and fintechs?

Opening a bank account in a country one does not reside in and/or where one's salary is not domiciled takes no more than a few minutes.

In fact, in most EU banks despite being an EU citizen, the following information is requested when trying to open a bank account as a local non-resident:

- Proof of employment (work contract or proof of company incorporation, if self-employed)
- Proof of registration (with the local authorities) within the country
- The regular set of information and documentation (usually consisting of an ID and a proof-of-address)

A temptation for criminals to abandon the traditional banking system

The recent media headlines will not contradict this fact: traditional banks are under strong pressure from the authorities to beef up their AML controls.

Emerging payments players from their ends—although they do not evolve in a lawless area since they need licenses (mostly payment institution or electronic money institution licences)—still take advantage of the EU regulation through the passporting mechanism, allowing them to operate in any European Economic Area while being supervised in another.

This consequently makes it much more difficult for both home and host regulators to supervise their activities across the EU, especially without an EU-wide supervisor. Financial criminals know this.

For example, a criminal could be willing to evade €100,000 of illegally obtained funds going through the easy account-opening process described earlier. Opening 10 accounts with 10 different fintech account providers, each licenced in different EU jurisdictions, would take them no more than 5-10 minutes per account with a smartphone and an ID. Now, even if the fintech does its job in terms of anti-money laundering/counter-terrorist financing (AML/CTF) measures, there is a high probability that the criminal would not be asked for more information nor documentation if they deposit up to €10,000 in each of these accounts.

Going one-step further, imagine that the amount to be evaded by the criminal would no longer be €100,000, but rather €1,000,000. The criminal would still open 10 different accounts at 10 fintechs, again each licenced in different EU jurisdictions, but instead of depositing €10,000 in each, they would deposit €100,000 structured into several smaller deposits.

Hopefully, this would trigger alerts within the fintech's monitoring systems. The criminal may even be asked to justify the source of these funds with further documentation. On top of that, the AML teams of fintechs may even fill and submit a suspicious activity report (SAR) to their local financial intelligence unit (FIU), but then what?

Ten different FIUs located in 10 different EU jurisdictions may be notified independently that one individual is conducting structured depositing into a licenced fintech account (e.g., Types of licenses: PI, EMI, specialised bank), within their jurisdiction.

Given the current workload of FIUs across Europe, the chances of a further investigation being triggered based on this piece of information—in isolation of what may have happened in other European countries—is very low.

Moreover, local FIUs within the EU still cannot rely on an EU-wide FIU that would centralise the information received from across member states.

Now the financial crime risks that these fintech/challenger banks pose are clear through the ease of opening multiple accounts all over Europe in a matter of minutes.

One can virtually open as many accounts as there are fintech providers able to do so

Virtual assets: A legal uncertainty that benefits criminals

Imagine that the fintech account providers discussed are, for the most part, regulated entities and as such, must abide by the same AML/CTF requirements as regular banking institutions. This is not yet the case across the EU for virtual asset providers (exchanges, wallet providers, etc.). Consequently, the following measures considered for fintech providers may not necessarily be applied by these players:

- KYC/customer due diligence
- AML/CTF transaction monitoring
- SARs

In fact and fortunately, the main virtual assets providers already do so. This does not just happen because these are "nice people" but because without it, they would have little to no chance of working with any of the financial institutions they partner with (acquiring banks, commercial banks, etc.) to facilitate their activity.

What are the possible solutions to tackle this new threat?

From the authorities' perspective

Despite the successive versions of EU AML Directives—since there are still quite a lot of differences among member states in terms of AML/CTF regulations and their enforcement—the EU passporting system could actually be weakening the overall AML/CTF measures.

To mitigate the risk of dirty money circulating via various online payment players that are sometimes not very vigilant and/or sufficiently controlled, one of the solutions would be for EU authorities to strengthen the powers of national supervisors. In addition, the creation of a common EU-wide supervisory body could allow the transition from a somewhat standardised regulatory framework to a possibly more standardised law enforcement policy.

From the fintechs' standpoint

As previously mentioned, the typical use of fintech accounts is as a complementary account rather than as a main account. Therefore, monitoring patterns and alerts can be subsequently designed.

As an example, if it is known that most customers fund their fintech accounts with their regular bank account and then use the balance to initiate direct in-app transfers to their friends and family, then questioning those who only receive funds from accounts they do not own (which they directly transfer to other accounts) without making any other use of fintech products makes sense.

Conclusion

Fintech account providers (fintechs) and emerging payment systems are fascinating in that they are demystifying financial products, opening the competition in the financial services' ecosystem (which was closed for a long time) and are ultimately putting customers back at the heart of the service provision.

Nevertheless, technology, innovation and disruption must not make one forget that these rising players are still fairly new when it comes to having a "culture of compliance" or operating within ever-evolving regulatory environments.

The typical use of fintech accounts is as a complementary account rather than as a main account

Thus, while regularly discovering new weaknesses and failures of well-established EU banking institutions, do not forget that these new entrants, as positive and well-intentioned as they might be, should also be closely monitored.

Alexandre Pinot, CAMS, head of Vilnius office and MLRO, SONECT Europe, Vilnius, Lithuania, alexandre@sonect.ch

[1] "EY Fintech Adoption Index 2017: The rapid emergence of Fintech," EY, 2017, https://www.ey.com/Publication/vwLUAssets/ey-Fintech-adoption-index-2017/$FILE/ey-Fintech-adoption-index-2017.pdf

[2] "Neo and Challenger Bank Customer Base to Grow by 50.6%, Globally, by 2020," Allied Market Research, https://www.alliedmarketresearch.com/press-release/neo-and-challenger-bank-market.html

[3] Oliver Smith, "A Million U.K. Consumers Just Switched Their Bank Accounts—But Not To Fintech Challengers" *Forbes*, 26 July 2018, https://www.forbes.com/sites/oliversmith/2018/07/26/a-million-u-k-consumers-switched-their-bank-accounts-but-not-to-fintech-challengers/#7932444c1205

[4] "Deposit guarantee schemes," European Commission, https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/managing-risks-banks-and-financial-institutions/deposit-guarantee-schemes_en

[5] Jeff Desjardins, "How Fintech is Digitally Disrupting the Financial World," Visual Capitalist, 3 August 2016, https://www.visualcapitalist.com/how-Fintech-digitally-disrupting-financial-world/

The intersection of AI in financial crime compliance

Artificial intelligence (AI) is the latest technology to take the compliance community by storm when it comes to reducing false alerts in both anti-money laundering (AML) and international sanctions screening programs. As European institutions begin to explore these technologies, many institutions are finding that the results do not always meet expectations.

Many AI algorithms operate as a "black box," delivering results with little explanation of how and why those results are produced.

Without explainability—also called interpretability—it is difficult for users to provide rationale on the model's results, which can render the model's output useless. In addition, institutions run the risk of unknowingly implementing biased models, which may run afoul of regulatory requirements for the following reasons:

- Inaccurate results are produced: In the area of financial crime that can mean missed sanction hits or undetected suspicious activity.
- Compliance gap: The inability for a firm to explain, validate or operationalise a model. In a context where both auditors and regulators are increasingly demanding in terms of model validation (as notoriously put forth by New York State Department of Financial Services Part 504).

On the other hand, traditional statistical methods may be blunt instruments when compared to modern AI techniques. They are cheaper and more explainable making them less risky solutions, which may be more acceptable to risk-averse organisations. Other organisations will likely combine AI with business rules for an optimal solution. More importantly, institutions need to understand what AI is in order to apply it to real business problems.

What is AI?

There are a number of different techniques that fall under the AI banner such as neural nets, random forests and support vector machines, among many others. Each have strengths and weaknesses and some techniques are more explainable than others.

Neural networks are an example of an AI technique where it is difficult to explain how the model came to the results.[1] It takes a lot of reverse engineering to determine how a neural net model produced a result. While some fuzziness or errors in an application—such as image recognition—might be acceptable for image classification models, financial institutions must meet a higher regulatory bar.

Requirements based on model risk-management guidance from the U.S. Federal Reserve (SR 11-7)[2] offers some best practices in managing risk associated with AI models. This includes documenting the model development, implementation and use, model validation, model governance and control. European regulators are also working to advance regulations around the use of AI models.

In the European Union (EU), General Data Protection Regulation (GDPR) requirements mean AI models processing personal data must be transparent. According to Capgemini, "This standard of accountability that companies must achieve will increase the standard of AI neural networks and force all of us to use an AI we can understand and control."[3] There must be a clear line of sight from data inputs to model outputs—inputs and outputs have to be explainable. Institutions and vendors in Europe need to pay particular attention to consumer

rights, opt-ins/opt-outs and effects on training and implementation of AI models in light of their GDPR obligations.

What is explainability?

It is helpful to define what explainability really means. The following are a few key features of explainability:

- The outputs of the model can be interpreted easily by non-technical users
- Components of the score can be easily identified
- The objectives of the model should map directly to results to satisfy regulatory oversight

For example, an AI model that is trained to score entity matches should include insight into what components of the entity are matched and how strong that match is. End users should be able to understand why a high or low score is generated and should be able to focus on the margins where the model cannot make a determination. If end users cannot understand the outputs of the model and be able to explain those results to others, they will not trust the results and may end up circumventing the model's decisions when they should not be circumvented.

McKinsey outlines an example where relationship managers could not understand cross-sell recommendations and thus ignores the model's recommendations.[4] This means all the resources obtained for training a model can go to waste if no one actually uses the results.

Using AI in AML and sanctions screening programs

In the financial crime compliance space, AI techniques are generally used in entity resolution—name matching—for watchlist screening and transaction monitoring for suspicious activity. This means an explainable model implemented for matching names should be able to surface the end-user entity. This includes attributes that match or nearly match reference data, how close the match is and how different identity elements contribute to the model's final score.

Similarly, for AML transaction monitoring a solution should be able to highlight reason codes indicating why a transaction or series of transactions are deemed suspicious. These explanations guide the end user to fully evaluate the alert activity and make a final decision on the activity.

While explainability is of great value for operational users, it is even more important when working with regulators. Regulators want to know that models work as intended and expect a validation process to ensure the models' effectiveness and applicability to a given problem. If the model is not explainable, it is very difficult to justify to regulators that it is working as intended.

Again, some AI techniques are more explainable than others and it is important for an institution to understand and set clear requirements on the explainability features in a solution, before making a technology decision.

An example could be in entity resolution, where the model may be biased toward or against different naming conventions such as Latin family name constructions, Asian naming conventions or Arabic patrilineal naming conventions. Much like statistical models, AI models can suffer from overfitting if the training data is not diverse enough.

Institutions should have a sound vendor selection process that includes requirements on the explainability of their models early in the buying process, starting with the request for information (RFI) or request for proposal (RFP). This is true for both AI and traditional statistical models.

An RFI and/or RFP could include open-ended questions such as:

- How are model outputs explained to end users?
- How are model outputs mapped to actual outcomes?
- How are models validated before entering production?
- What efforts are in place to reduce bias in the model?
- Can an end user interpret and explain the score/decision output by the model to a customer or regulator if necessary?

This is not an exhaustive list, but open-ended questions like these can help an institution evaluate how an AI solution will fit into existing operational flows and model risk-management practices. There may be some new model risk-management practices that apply specifically to AI models. In fact, McKinsey identified six new components for validating AI models compared to traditional models.[5] These include feature engineering, hyper parameters, interpretability (explainability), bias, production readiness and dynamic model calibration.

The promise of AI is very real in the financial crime compliance space, but these techniques may not be an ideal fit for every challenge. In some instances, more traditional analytical models can provide higher-quality results that are easily explainable. In other cases, it may be a combination of AI techniques, statistical models and business rules that provide the most defensible, accurate and targeted results.

Every organisation is unique, but every organisation can benefit by asking the question: "Could you please explain the outputs of the model?"

Michelle McCann, Ph.D., global head of portfolio marketing, Accuity, London, U.K., michelle.mccann@accuity.com

[1] Gregory Barber, "Shark or Baseball? Inside the 'Black Box' of a Neural Network," *Wired,* 6 March 2019, https://www.wired.com/story/inside-black-box-of-neural-network/

[2] "SR 11-7: Guidance on Model Risk Management," 4 April 2011, Federal Reserve Board, https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm

[3] Nikolai Horn and Pierre-Adrien Hanania, "AI and the Janus face of the GDPR – chance or challenge?" Capgemini, 30 November 2018, https://www.capgemini.com/2018/11/ai-and-the-janus-face-of-the-gdpr-chance-or-challenge/

[4] Bernhard Babel et. al, "Derisking machine learning and artificial intelligence," McKinsey & Company, February 2019, https://www.mckinsey.com/business-functions/risk/our-insights/derisking-machine-learning-and-artificial-intelligence

[5] Ibid.

THE RISE OF cloud IN COMPLIANCE

The last 18 years have seen financial institutions (FIs) create and deploy money laundering detection and prevention defences in response to regulatory demands. The means by which FIs achieve this task have stayed the same for decades. Institutions will go to the market, scan providers with solutions, select and purchase one, deploy it on an on-premises infrastructure and then run the solution. This strategy works well and has allowed many FIs to successfully comply with regulations.

Although this approach works well, it is not perfect, leaving some institutions out of compliance, lacking in ability to detect and vulnerable to penalties. A key limitation is the deployment to on-premises infrastructure. FIs have to buy the hardware, mobilise an information technology (IT) team to set it up, deploy the software and monitor the correct execution of the solution on a daily basis. This involves installing a service desk to resolve level 1 user issues and support contracts with every vendor involved in the infrastructure (database, application server and so on), in order to correct bugs or get answers to questions.

All those activities and their subsequent costs are purely IT-related and have nothing to do with core compliance activities of FIs; they truly are a support function. Yet there are still solid reasons to stick with tradition and keep the existing target-operating model (TOM). The sensitivity of data processed, criticality of compliance activities and risk of fines if changes go wrong all represent strong incentives to maintain control with an on-premises solution, at least until recent years.

Now the pace has picked up, and the last two years have seen significant change that should give FIs reason to take a fresh look at their model. A key change is the emergence of mature public cloud providers with enhanced offerings that provide an opportunity for FIs to move from an on-premises compliance platform installation to software as a service (SaaS) hosted in a public cloud environment.

As it has happened with other, less critical applications, the benefits of moving to the cloud are starting to outweigh the potential drawbacks. The cost of failure for a compliance solution for most institutions is far more severe and far-reaching than webpage downtime or loss of web-chat customer services, yet other factors are conspiring to change the equation significantly in favour of cloud.

Cloud benefits

An important change is coming from FIs themselves as they accelerate their global digital transformation. An example of this is having the IT office able to deliver new services to the business in an agile approach and continuous basis. Compliance was initially protected from agility need, as regulations were slowly evolving. Over the last years, there has been both an increase in the number of relevant laws, such as the Fourth AML Directive, general data protection regulation (GDPR), Fifth AML Directive (implementation deadline approaching), and rapid policy and regulation changes—for example,

It is recognised that the key asset for FIs is data, and that this is a competitive advantage over their competitors

countries being placed on or removed from sanctions lists on a more regular basis. This rapid change has created the need to improve time to market (TTM) for tools and as such, the ability to quickly deploy a new change in production—a critical need for FIs.

The end-to-end process to deploy in production is a change requested by the business and it is often the bottleneck of the agility expected. Public cloud providers have optimised those processes to the extreme, as it is their core business. In addition, by moving to cloud, FIs offshore the complexity of this process and put the responsibility of success outside.

The increasing volumes of financial transactions require a constant adjustment to the size of the compliance platform infrastructure sometimes just to handle a couple of moments of peak seasonal demand, such as Christmas. Distributed architecture allows for scalable infrastructure, meaning when unused, the infrastructure is allocated to other solutions. However, to ensure such scalability, there needs to be an extremely high number of servers and a solution optimised for them as well. This is perfectly possible for well-resourced FIs but it requires many IT investments. To ensure high availability and performance of the compliance solution, the IT office has no choice but to size the infrastructure on the peaks, leading to an oversized infrastructure 90 percent of the time. As a result, the direct impact of this new volumetric is a direct increase in IT costs, with little opportunity to optimise without impacting the quality of service.

Cloud providers have two competitive advantages to any IT office of FIs:

1. They have farms of servers, all built in fully scalable architecture which gives them the capability to reallocate unused infrastructure to a different customer; as a result, there is no leakage due to peak activities.
2. Given the number of servers, they are able to both mutualise teams and procurement and as such—for a similar infrastructure—greatly reduce the total cost of ownership.

Coupled with a "per usage" pricing model, where FIs pay the servers only if they are actually using them, cloud providers are in position to propose an extremely competitive price to FIs in order to host their compliance solution. That also changes the category of costs, moving from capital expenditure (on-premises installation), to operating expenditure (when using a cloud provider). Used the right way, this difference will benefit most companies.

It is recognised that the key asset for FIs is data, and that this is a competitive advantage over their competitors. Therefore, they have always been extremely cautious in handling and disclosing it. For years, the initial reaction was to keep data on-premises (inside the walls of the company)—a fair statement. Public cloud providers struggled to defeat this mindset by being opaque and by not communicating the geography of their data centres to European customers. This makes it difficult to build trust or even to guarantee compliance with some local regulations, not allowing data to leave the country. Yet in the last few years, public cloud providers have made large progress on this and they are now providing a clear view of their servers' availability, zone and location. They keep increasing this offer and take the same into consideration when defining new availability zones.

Also, many large companies worldwide (not only FIs) have suffered from data breaches over the last years, resulting in reputational damage. None of the public cloud providers has ever suffered such a data breach, which could be a company-killer. It is in the interest of cloud providers to take every measure to ensure this will not happen.

FIs have been more cautious in deploying cloud solutions on uncritical activities that are outside of the compliance department

In addition, a company must have multiple intrusion scenarios and it needs to protect itself. Some of these scenarios can be an intrusion directly from the network, an intrusion from an external site and so on. For each identified risk, the company has to provide a different secure access like a virtual private network or reverse proxy and multiply the cost and complexity of maintaining a strong and resilient security policy. For a cloud provider, it is moving the cloud offshore. In addition to data breach risk, a company also needs to protect itself from natural disasters and similar events. That means setting up a disaster recovery plan with a recovery time objective and recovery point objective, which will also require investments to ensure an efficient recovery plan. This is part of the core offering of a public cloud provider.

Turnaround

In other regions, such as Asia and Oceania where data regulation has been much more flexible over the years, several FIs have already successfully moved to a SaaS approach. For example, they are using a full compliance solution including transaction monitoring, sanctions and politically exposed persons (PEPs) screening, and customer risk rating in SaaS mode, hosted by a well-known public cloud provider. This is working effectively and none of them are considering turning back to the on-premises hosted solutions.

In the specific context of Europe—given the much stricter regulation on data privacy highlighted by the enforcement of GDPR in May 2018—FIs have been more cautious in deploying cloud solutions on uncritical activities that are outside of the compliance department.

FIs are at a turnaround point on the market. While the red flags are being progressively removed, FIs are now having a closer look at the massive benefits they would receive from moving their compliance platform to a cloud environment. Some benefits include reduced IT costs, increased agility and TTM, and reduced IT complexity in order to focus on core business. For the last five years, compliance solutions being cloud compatible was a tick-in-the-box question. Now FIs dive deep into how they could deploy their compliance platforms in cloud environments. In an always competitive environment looking for process optimisation and cost reduction, moving to the cloud is the next step to consider. A

Rémi Demelle, CAMS, customer success manager, BAE Systems Applied Intelligence, Paris, France, Remi.Demelle@baesystems.com


BAR
BAR

SARs analysis on the criminal use of the gaming (casino) sector

A recent report written by the Metropolitan Police Service (MPS) examined the link between criminality and gambling. The MPS report analysed 250 suspicious activity reports (SARs) submitted by the gaming (casino) sector and other reporting sectors. Casinos are referenced between the 1 of January 2017 and the 30 of June 2017 within the MPS.

The analysis is considered necessary due to the extensive amount of time that has elapsed since the last Financial Action Task Force (FATF) report concerning "Vulnerabilities of Casinos and Gaming Sector" in 2009.

The MPS report predominantly focused on land-based casinos (although some betting shops and online gambling sites were also included within the sample).

The SARs were evaluated to ascertain whether or not those reported have a criminal record.

The analysis determined the level, gender and nationality of the criminals and identified whether any previous SARs had been filed for those individuals.

The report specifically considered the relevance of SARs-derived information in relation to the following issues:

- Are known criminals using casinos to launder and spend their criminal cash?
- What predicate offences have these known criminals committed?
- Are known criminals being reported by both the regulated financial sector and the gaming (casino) sector? Have variations in typologies for both sectors been compared for reporting?
- Does the percentage of criminals being reported by SARs support or contradict previous research?
- Are SARs reporting casino employees who might pose an insider money laundering threat to the industry?

- Is there a link between Scottish banknote usage in United Kingdom (U.K.) casinos and criminality?
- Is there confirmation that SARs benefit law enforcement agencies (LEAs) by providing immensely valuable intelligence to initiate investigations and identify potential and otherwise unknown criminals?
- Are SARs submitted following inquiries received from law enforcement (in effect the SARs system working in reverse?)
- Who requests payouts in large denomination notes and/or sealed in casino packaging?
- Have the individuals disclosed in the SARs been previously reported?
- Are those reported born within or outside the U.K.?

Key findings

The MPS findings show a positive correlation between SARs in identifying known criminals using casinos to spend criminal proceeds as part of their criminal lifestyle to either conceal or disguise the source of criminally derived cash.

Furthermore, SARs offer LEAs infinite opportunities to instigate investigations and identify potential and otherwise unknown criminals laundering the proceeds of their or others' criminality.

Analysis ascertained the following data:

- Two percent of the 250 SARs were submitted following a law enforcement inquiry
- Eight percent of those reported were employees working in casinos in the gaming sector
- Thirteen percent of the SARs were requests for a defence against money laundering (DAML) for a future activity that may constitute a prohibited act
- Thirty-two percent of the SARs provided by the regulated financial sector identified an individual with a criminal record
- Thirty-seven percent of those reported have a criminal record
- Forty-nine percent of the SARs submitted by the gaming (casino) sector identified an individual with a criminal record
- Fifty-two percent of those reported had been the subjects of previous SARs
- Sixty-two percent of those reported were born outside of the U.K.
- Eighty-seven percent of those reported who were involved in the expenditure or exchange of Scottish banknotes within U.K. casinos have a criminal record

Are SARs identifying known criminals?

The 250 SARs referenced 253 individuals. The MPS examined these 253 names against the Police National Computer (PNC)—a law enforcement database that contains the details of all persons arrested, convicted, cautioned or charged with a criminal or summary offence—to determine the extent to which they corresponded to known individuals.

The results revealed that 95 of the 253 persons or 37 percent identified by the SARs had a criminal record. Twenty-seven of these 95 were prolific/career criminals who altogether had convictions for 400 offences. (In this interpretation, career criminals are those with 10 or more criminal convictions, in addition to numerous other arrests and court appearances that for various reasons did not result in a criminal conviction.)

Thirty-two percent of the SARs provided by the regulated financial sector identified an individual with a criminal record

The 25 different types of crimes identified from the 400 offences included murder, kidnapping, possession of firearms, perverting the course of justice and threats to kill.

These are serious criminal offences and they indicate that an individual is involved in a serious organised crime.

The most common predicate offence for known criminals using casinos was fraud followed by theft offences, criminal damage and burglary.

The most common offence committed by the majority of the 27 prolific offenders was violence-related, whereby 18 had convictions for assaults and battery. Nine of these 27 also had convictions for money laundering.

Comparison between the SARs submitted by the regulated financial sector and gaming (casino) sector

A review of the SARs submitted identified variations in reporting reflecting the specific requirements of contrasting businesses and the subsequent individual approach they have adopted to identify, assess, understand and mitigate the money laundering and terrorist financing risks.

Financial institutions revealed the following suspicions of money laundering:

- Cash credited to an account, the source of which was unknown and debits funded to casinos/gambling organisations
- Accounts that fund excessive gambling, especially if they were listed as students
- Employees in senior manager positions where accounts revealed high expenditure/debits to casinos/gambling organisations
- Casino employees in receipt of unidentified cash credits or who gambled large amounts of money
- Individuals named in inquiries conducted by LEA and other public sector organisations in relation to criminal investigations
- Deposits of large amounts of cash sealed in casino packaging
- Individuals in receipt of government benefits who gamble excessively
- Individuals who appear to be living beyond their means
- Bank staff who resort to payday loans to gamble

On the other hand, casinos and those involved in the gaming (casino) sector reported the following suspicions of money laundering:

- Withdrawing funds on bank/credit cards indulged in limited play within a short duration and then cashing out
- Feeding cash into gaming machines and cashing out after minimal play, requesting £50 notes in sealed casino packaging
- Politically exposed persons (PEPs) with cash sums in large denominations
- Heavy monthly losers that exceed a certain threshold, i.e., £50,000 per month
- Individuals who attend and spend Scottish banknotes in English casinos
- Exchanging large cash amounts to play
- Attempting to exchange lower denomination notes into £50 notes
- Barred members who are identified when they attempt to cash out
- Customers with no recorded play who exchange casino chips for cash

Analysis indicated that casinos rarely use SARs to report money laundering suspicions relating to their own staff—despite evidence to suggest that money laundering offences can be committed by both customers and casino employees.

In comparison, the regulated financial sector reports both their own employees and casino employees who appear to be living beyond their means. This is highlighted by the fact that 23 of the 250 SARs submitted reported money laundering suspicions against 21 employees working within the casino industry.

Financial institutions submitted all of these SARs relating to casino employees. Five of the 21 casino employees reported had criminal records, with two of these five being prolific career criminals and one having appeared in court on nearly 30 occasions.

Others mentioned in the SARs were gambling significant amounts not commiserate with their salaries. This raises a number of important questions. How is this gambling funded? Could they be involved in internal fraud or other unknown criminality? Are they a threat to the relevant organisation?

This implies that an insider may cause the same money laundering threat as a customer and therefore it is essential that an institution instigates an effective know your employee (KYE) programme that vets staff members.

This vetting process should be ongoing, as employees' circumstances change over time, with some succumbing to crime due to personal and financial problems.

The findings suggest that the gaming (casino) sector's KYE programme may require developing or adjusting to reduce the risk of a potential insider money laundering threat that could have a devastating effect on the industry.

Is there a link between Scottish banknote usage in U.K. casinos and criminality?

Alternatively, only casinos in England appear to report those who spend or exchange Scottish banknotes.

Eight of the 250 SARs made specific mention of customer's usage of Scottish banknotes. Seven of these eight had criminal records, with four being prolific offenders.

All were male and all exchanged the notes for Bank of England banknotes or fed the Scottish notes into gambling machines, and engaged in minimal play before cashing out and receiving Bank of England banknotes.

Half had travelled from their London address to casinos situated in the north to launder these potential criminal funds.

Analysis indicated that casinos rarely use SARs to report money laundering suspicions relating to their own staff

Are the SARs submitted by the regulated financial sector and gaming (casino) sector identifying known criminals?

How did the casino and others in the gambling sector compare to the regulated sector in identifying those 95 criminals of most interest to LEAs?

The regulated sector provided 136 of the 250 SARs analysed; 44 of these 136 SARs or 32 percent identified 30 persons known to the PNC.

The casino and gambling sector provided 111 of the 250 SARs analysed; 54 of these 111 or 49 percent identified 45 persons known to the PNC.

Both appear to be impressive figures and this analysis powerfully suggests that SARs can suggest criminality, making them of immense value to LEAs.

Finally—and of great interest to LEAs for future planning in the Pursue, Prevent, Protect and Prepare strategy—the SARs were also analysed to ascertain where the 75 criminals known to the PNC reside in London.

The highest number, 26 of the 75 or 34 percent, reside in east London followed by 13 of the 75 or 18 percent in northwest London and nine of the 75 or 12 percent in west London.

The initial perception relating to persons unknown to LEA databases is that these are innocent, law-abiding members of the public

The SARs that relate to persons unknown to the PNC

In attempts to measure the value of SARs, studies and reports frequently concentrate on comparisons with known individuals to demonstrate the value of intelligence produced. The initial perception relating to persons unknown to LEA databases is that these are innocent, law-abiding members of the public.

A different interpretation of this analysis is that 158 of the 253 persons identified, or approximately 63 percent, are not known to the PNC. This suggests that 152 of the 250 SARs submitted are not suspicious, thereby casting serious doubts about the quality of suspicion contained within the majority of reports provided by the gaming and regulated sector and regulated financial sector.

Many of the SARs submitted on individuals unknown to PNC were in receipt of large cash payments that were subsequently gambled. These individuals were in low salary occupations or listed as students. These account credits are substantial—for example: amounts of £118,000, £77,000, £70,000, £64,000, £54,000 and £49,000 were reported in this analysis. Those on a high salary may be able to lose £50,000 within a period of one to two months, but can someone on benefits, who is unemployed or is earning £12,000 to £15,000 a year afford such losses? Is it their cash? What is the source? What is the predicate offence?

Others are reported for paying cash into machines to gamble and either not gambling or gambling a minimal amount within a short time period before cashing out the same amount or a much larger amount (with chips, plaques, etc., which they have not purchased). This suggests placement and layering of suspected criminal funds and people attending casinos on behalf of others whose identity is unknown.

Interestingly, the SARs evaluated indicated that those who did not have a criminal record were more likely than those who had a criminal record to request high denomination £50 notes and sealed casino packages.

Have the individuals disclosed by the SARs been previously reported?

In addition to examining the value of casino-related SARs against the PNC, this report explored whether any other SARs were made against the subjects identified and if they had been reported by different reporting entities.

The individual details of the 253 persons identified by the SARs were put into the ARENA database (a search and analysis tool for end users of SARs) to ascertain those that had been previously disclosed by reporters.

The analysis revealed that 130, or 52 percent, of the sample had been the subjects of previous disclosures with a further 248 SARs submitted on these individuals.

There was a total of 498 SARs related to these 253 individuals, with 215 of the 498 SARs relating to the 95 with a criminal record and the remaining 283 referring to the 158 not known to the PNC.

Nationality, criminality and gender of the subjects of the 250 SARs

The information provided within the SARs was also analysed to review the purported nationality, ethnicity and gender of those being disclosed. Based on the information provided the results were as follows:

- The individuals disclosed provided documentation indicating that they originated from 51 separate nations. The 95 individuals known to the PNC originated from 29 different jurisdictions.
- The analysis revealed that of the 95 individuals known to the PNC, the majority purportedly came from the U.K. (34), followed by seven from Pakistan and seven from China and four each from Afghanistan, Albania and Vietnam.
- The largest nationality reported were those born in the U.K. (65 percent or 25 percent of the total) and over half of these were known to the PNC.
- However, one of the most striking findings was that 158 of the persons reported, or 62 percent, provided documentation to indicate that they were born outside of the U.K.
- These findings must be interpreted with caution because 30 of the total 253 individuals reported, or 12 percent, did not indicate a nationality.
- Casinos made 23 of these reports.
- This suggests a failing in some reporters customer due diligence (CDD) process. This is significant as knowledge underpins the entire anti-money laundering/counter-terrorist financing (AML/CTF) compliance structure. The more an institution knows about their customers, the greater the chance of preventing money laundering.
- In addition, 46 of those reported had no known occupation nor indicated an employer. This might suggest a lack of understanding of the money laundering risk as information concerning the purpose and nature of the business relationship appears to be insufficient. Or are institutions allowing potential language difficulties to get in the way of proper questioning to obtain the prerequisite CDD requirements?

Either way this lack of accurate customer identification demonstrates inadequacies in CDD, AML/CTF programs and an institution's compliance regime.

Conclusion

Research suggests that criminals use casinos to place, layer and spend criminal funds. In addition, the gaming (casino) sector and the regulated financial sector appear to be recognising and identifying suspicious activity by their customers.

SARs provided by the gaming (casino) sector suggest that nearly 50 percent of those reported have criminal records. These figures are significant as they are much higher than previous research indicated and clearly illustrate the depth of criminal use of casinos and betting within the gambling industry.

These results are significant because they suggest that SARs make a positive contribution to the work of law enforcement, and are a powerful weapon in the investigation and fight against money laundering and other crime. A

Graham Edwards, detective constable, Metropolitan Police Service, London, U.K., Graham.edwards3@met.pnn.police.uk

An inspection of the real estate sector in Germany

Germany's real estate industry is one of the largest economic sectors of the country, with 817,000 companies and around 3 million registered employees in 2017. In 2016, the entire sector was valued at around €500 billion, representing a contribution of 18.2 percent to the growth of the entire economy.[1]

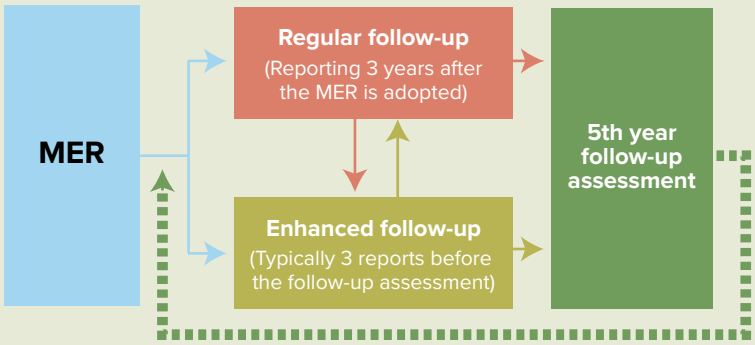
It is understandable that within this context, this sector would present an attraction to those seeking to launder illegal financial resources. A 2018 report by Berlin-based nongovernmental organization Transparency International estimated that 15-30 percent of criminal assets are invested in real estate. In 2017, around €30 billion of suspicious funds were reportedly moved through the sector.[2]

The numbers are impressive and they raise doubt on how effective Germany's strategy is in dealing with money laundering more broadly, particularly in the property sector. The goal is to analyse the phenomenon by answering three questions:

1. What is the current state of Germany's anti-money laundering (AML) legislation?
2. Who are the actors involved with money laundering in German real estate?
3. How could Germany's AML efforts be improved?

Regulatory and institutional state of affairs

A good indication of Germany's challenges in developing a decent AML regulatory system is provided by the mutual evaluation reports (MERs) from the Financial Action Task Force (FATF), the world's leading body in the field.



Source: "Mutual Evaluations," Financial Action Task Force, http://www.fatf-gafi.org/faq/mutualevaluations/

In February 2010, FATF concluded in Germany's MER that Germany was susceptible to money laundering and terrorist financing because of its large economy, financial centre, strategic location in Europe and strong international exposure. An estimated €40-60 billion in criminal proceeds was generated annually in the country. Furthermore, Germany's AML/counter-terrorist financing legal framework was not aligned with FATF Recommendations. An example of this was the pursuit of money laundering crimes through predicate offences[3] that required a higher burden of proof. In addition, German authorities had not been able to confiscate property due to limitations[4] on their ability to locate property.[5]

In June 2014, FATF decided to remove Germany from the regular follow-up process due to a lack of progress in addressing the issues identified in 2010. Germany had amended the criminal code by including insider trading, market manipulation, counterfeiting and piracy of products as predicate offences to money laundering. Nevertheless, the issue of asset freezing had not been addressed at the time.[6] The next round of MERs is due around October/November 2020.

Since 2014, a series of steps have been taken to improve Germany's AML efforts. In June 2017, a new national AML law (Geldwäschegesetz) entered into force, which implemented the Fourth AML Directive.[7] In addition to a strong emphasis on enhanced due diligence, the new German regulation introduced a so-called transparency register (Transparenzregister) focused on the ultimate beneficial ownership of companies.[8] By June 2018, 3,132 applications out of a total 55,504 entries had been submitted for inspection. Nevertheless, in the property sector, registrations had been incomplete or avoided altogether.[9]

Along with a companies' register, a transparent database for property owners is needed. As of today, German land registers are within the responsibility of the local courts, with each district running the land register in the area. The establishment of a public and centralised real estate register (Immobilienregister) has been requested by a variety of political actors ranging from the Green Party[10] to the Social Democratic Party of Germany, the partner of the Christian Democrats in the current governing coalition.[11]

Another promising measure adopted in July 2017 was the transfer of the financial intelligence unit (FIU), the country's AML organism, from the Ministry of the Interior (Federal Criminal Police Office) to the Ministry of Finance (customs office). The decision was justified by the latter's apparent success in fighting drug smuggling and performance in the area of international cooperation.[12] In October 2018, head of the FIU Christof Schulte warned specifically against an increase in criminal activities in the real estate sector, predicting that the FIU's staff would increase in 2019 from 360 to 475 employees. The results from the reformed FIU have been widely criticised thus far. Schulte noted that in 2017, decisions had been made for only 474 court cases. In addition, out of almost 60,000 suspicious transactions reported that year, only about 20 had been filed by real estate agents.[13] The difficulty in recruiting much-needed personnel due to the FIU's unattractive employment conditions is aggravating.[14]

Regarding the highly discussed issue of criminal asset recovery, a new law[15] was introduced in July 2017 with the goal of facilitating the temporary seizure of assets and their subsequent liquidation.[16] A crucial aspect of the new regulation is the reversal of the burden of proof. Following the Italian model employed in the fight against the mafia, authorities can now confiscate the assets of a suspect, unless the origin of that asset can be proven. Previously, the state had to prove the illicit origin of the asset.[17] However, difficulties still exist upon close inspection. Critics talk of a "traffic jam" of enforcement titles, meaning that the enforcement of the court-ordered confiscations is rocky due to insufficient personnel. In addition, criminals no longer hold the stolen assets, and confiscations mostly result in a high number of private bankruptcy petitions.[18]

The Italian mafia, Arab clans and clandestine Russian interest

A February 2019 article by *Süddeutsche Zeitung* reported that Italian criminal organizations like the Camorra and the 'Ndrangheta had been profiting from the rising real estate prices in Munich. A 2017 tapped telephone conversation between mafia members regarding their intent to purchase any kind of property in Germany was used to support the above allegation.[19]

In November 2006, the media reported on a "secret study" by the German foreign intelligence service

which showed that the 'Ndrangheta had been investing millions of euros in German hotels, restaurants and houses, especially along the Baltic coast and in the German states of Thuringia and Saxony.[20]

The presence of Italian criminal groups and their participation in money laundering activities in German territory is common knowledge at this point. For example, an Italian small business owner was on trial in Cologne in April 2014, following indictments for using a network of 17 construction-related businesses to help launder money for a fee. This case raised questions whether the Italian mafia might be involved. An investigation by Westdeutscher Rundfunk (a German public broadcaster), *Funke Mediengruppe* (a German newspaper publisher) and the news magazine *Der Spiegel* confirmed these suspicions. German authorities shared the same assessment.[21]

Later on, in December 2018, a series of raids against the 'Ndrangheta took place in Germany, Italy, Netherlands and Belgium under the code name "Pollino." In Germany, the operation took place in Bavaria and in North Rhine-Westphalia, resulting in 15 arrests. Money and valuables worth about €5 million were seized. The accusations against the suspects were for trafficking cocaine and money laundering.[22]

Arab clans have also been involved in the phenomenon. For example, in Berlin in July 2018, 77 properties worth €10 million belonging to a Lebanese-born clan were confiscated as its members had been suspected of having acquired the real estate with money obtained from various crimes including robbery, drug trafficking and even murder. Above all, there was suspicion that three of the family members had been involved with the theft of a 100-kilogram gold coin worth €3.7 million from the Berlin Bode Museum in July 2017. However, the seizure of the real estate is provisional and the family members can continue to live in the properties. Whether the court in Berlin decides to permanently withdraw the properties from their owners remains uncertain.[23]

Russian clandestine interests are also striving for a share in this booming industry. Despite having been in the European Union sanctions list since 2014, Russian oligarch Arkadi Rotenberg is allegedly a close associate of Russian President Vladimir Putin. In May 2018, the German media reported him as being the ultimate beneficial owner of the following properties in the country: Opernpalais in Munich, LES 1 office complex in Hamburg, Sofitel Frankfurt Opera Hotel in Frankfurt and Kudamm-Karree in Berlin. These properties were thought to be worth €1 billion.[24]

In February 2019, following a three-year-long investigation, German authorities announced the seizure of four properties worth €45.39 million in southern Germany in relation to the so-called "Russian Laundromat,"[25] an international money laundering scheme involving €22 billion illicit funds being moved out of Russia between 2010 and 2014.[26]

Policy recommendations

Following the analysis presented so far, some suggestions for improving Germany's AML efforts could be put forward. A good starting point for this could be the 2018 Transparency International report mentioned herein.[27]

Primarily, enhanced due diligence is indispensable. It has been claimed that real estate agents, notaries and lawyers insufficiently examined their clients in terms of political affiliation or origin of funds. Legal experts also underscore the importance of due diligence in protecting real estate companies against money laundering.[28]

Secondly, foreign companies that owned real estate in Germany should have to report their beneficial owners to the transparency register. In addition, a centralised land register should be established and made public.

Finally, sufficient resources must accompany new legislation and institutions such as the asset recovery law and the FIU. Moreover, prosecutors and police should be in a position to investigate money laundering independently of other predicate offences.

Given the looming FATF review, due to take place in 2020, Germany needs to make significant improvements to its AML regime in order to avoid reputational repercussions. A

Claudiu-Nicolae Sonda, analyst, Berlin Risk Ltd., Berlin, Germany, claudiu.sonda@berlinrisk.com

[1] "Die deutsche Immobilienwirtschaft—Stabilisator und Wachstumsmotor," ZIA, https://www.zia-deutschland.de/marktdaten/daten-der-immobilienwirtschaft/

[2] Alistair Walsh, "German real estate market a hotbed of money laundering, Transparency reports," Deutsche Welle, 12 July 2018, https://www.dw.com/en/german-real-estate-market-a-hotbed-of-money-laundering-transparency-reports/a-46637937

[3] For example, financing of terrorist acts.

[4] For example, professional secrecy.

[5] "Anti-Money Laundering and Combating the Financing of Terrorism Germany," Financial Action Task Force, 19 February 2010, http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20Germany%20full.pdf

[6] "3rd Follow-up Report Mutual Evaluation of Germany," Financial Action Task Force, June 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/mer/FUR-Germany-2014.pdf

[7] "Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance)" EUR-Lex, 20 May 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849

[8] "Controversial German Anti-Money Laundering Law," Global Risk Affairs, 10 July 2017, https://www.globalriskaffairs.com/2017/07/controversial-german-anti-money-laundering-law/

[9] "Behörden nutzen neues Anti-Geldwäsche-Register kaum," Der *Tagesspiegel,* 26 June 2018, https://www.tagesspiegel.de/politik/transparenzregister-behoerden-nutzen-neues-anti-geldwaesche-register-kaum/22735888.html

[10] Lisa Paus (Member of the German parliament),"PM Geldwäsche-Aufsicht im Immobiliensektor ist ein Witz," 18 June 2018, https://lisa-paus.de/2018/geldwaesche-aufsicht-im-immobiliensektor-ist-ein-witz-2/

[11] "Antrag 59/II/2018 Transparenz auf dem Immobilienmarkt herstellen—Offenes Immobilienregister einführen," SPD Berlin, 12 October 2018, https://parteitag.spd-berlin.de/cvtx_antrag/transparenz-auf-dem-immobilienmarkt-herstellen-offenes-immobilienregister-einfuehren/

[12] "Zoll soll Geldwäschern das Leben schwer machen," *Handelsblatt,* 4 April 2017, https://www.handelsblatt.com/politik/deutschland/bundeskriminalamt-zoll-soll-geldwaeschern-das-leben-schwer-machen/19615190.html

[13] "Anti-Geldwäsche-Einheit warnt vor kriminellen Machenschaften bei Immobilien," *Spiegel Online,* 17 October 2018, http://www.spiegel.de/wirtschaft/soziales/immobilien-anti-geldwaesche-einheit-warnt-vor-kriminellen-machenschaften-a-1233662.html

[14] Jan Keuchel, "Geldwäsche in Deutschland—ein Staat verliert die Kontrolle," *Handelsblatt,* 27 February 2019, https://www.handelsblatt.com/politik/deutschland/kaum-ueberwachung-geldwaesche-in-deutschland-ein-staat-verliert-die-kontrolle/23120348.html?ticket=ST-1697212-ke3wiKyklzJt3fqhzsLT-ap2

[15] In German, Gesetz zur Reform der strafrechtlichen Vermögensabschöpfung.

[16] "Überblick zur Neuregelung der strafrechtlichen Vermögensabschöpfung zum 01.07.2017," Anwalt.de, 22 May 2017, https://www.anwalt.de/rechtstipps/ueberblick-zur-neuregelung-der-strafrechtlichen-vermoegensabschoepfung-zum_106897.html

[17] "Gesetz zur „Vermögensabschöpfung" potenzieller Krimineller," Welt.de, 19 July 2018, https://www.welt.de/newsticker/dpa_nt/afxline/topthemen/hintergruende/article179643370/Gesetz-zur-Vermoegensabschoepfung-potenzieller-Krimineller.html

[18] "Berlin will 40 Millionen Euro von Kriminellen einziehen," *Der Tagesspiegel,* 3 August 2018, https://www.tagesspiegel.de/berlin/vermoegensabschoepfung-berlin-will-40-millionen-euro-von-kriminellen-einziehen/22879698.html

[19] Martin Bernstein, "Nutzt die Mafia den Immobilienboom zur Geldwäsche?" *Süddeutsche Zeitung,* 21 January 2019, https://www.sueddeutsche.de/muenchen/mafia-muenchen-immobilienmarkt-1.4297114

[20] "Italian Mafia Invests Millions in Germany," *Deutsche Welle,* 13 November 2006, https://www.dw.com/en/italian-mafia-invests-millions-in-germany/a-2237523

[21] Jörg Diehl, "How the Italian Mafia Is Infiltrating Germany," *Spiegel Online,* 8 April 2014, http://www.spiegel.de/international/germany/sicilian-mafia-infiltrates-german-construction-business-a-963194.html

[22] "15 Festnahmen nach Razzien gegen Mafia in Deutschland," *Süddeutsche Zeitung,* 5 December 2018, https://www.sueddeutsche.de/panorama/mafia-razzia-deutschland-ndrangheta-1.4239833

[23] "Immobilien eines arabischen Clans im Millionenwert beschlagnahmt," *Zeit Online,* 19 July 2018, https://www.zeit.de/gesellschaft/zeitgeschehen/2018-07/berlin-grossfamilie-clan-immobilien-diebstahl-toetungsdelikte-drogenhandel

[24] "ARD-Magazin 'Plusminus' meldet: Putin-Freund kauft heimlich deutsche Immobilien auf," *Focus,* 16 May 2018, https://www.focus.de/immobilien/kaufen/ard-magazin-plusminus-putin-freund-arkadi-rotenberg-kauft-heimlich-deutsche-immobilien_id_8939868.html

[25] "The Russian Laundromat," Organized Crime and Corruption Reporting Project, 22 August 2014, https://www.occrp.org/en/laundromat/russian-laundromat/

[26] "Germany Seizes 50 Mil Euros of Russian Laundromat Loot," Organized Crime and Corruption Reporting Project, 21 February 2019, https://www.occrp.org/en/daily/9269-germany-seizes-50-mil-euros-of-russian-laundromat-loot

[27] "Massives Problem mit Geldwäsche bei Immobilien—Politik, Wirtschaft und Behörden müssen endlich offensiv handlen," Transparency International, 7 December 2018, https://www.transparency.de/aktuelles/detail/article/massives-problem-mit-geldwaesche-bei-immobilien-politik-wirtschaft-und-behoerden-muessen-endlich-off/

[28] Peter Fissenewert, "Geldwäsche: Risikofaktor für die Immobilienbranche," Buse Heberer Fromm, November 2016, https://buse.de/insights/geldwaesche-risikofaktor-fuer-die-immobilienbranche/

Risky business: 5AMLD and EDD

The Fifth European Union (EU) Anti-Money Laundering (AML) Directive (5AMLD)[1] which entered into force on the 9 of July 2018, must be implemented by the EU member states by January 2020. Firms affected by the new directive, obliged entities, face new challenges resulting from the relevant amendments to the Fourth EU AML Directive (4AMLD) of 2015 (implemented in 2017).[2]

Business relationships with high-risk third world countries, countries assessed by the European Commission as having strategic deficiencies in their anti-money laundering/counter-terrorist financing (AML/CTF) regimes, are of particular concern.[3] The new directive imposes enhanced due diligence (EDD) requirements and suggests possible business restriction with respect to these high-risk countries (see box 2).

However, the selection of countries for the blacklist has proven to be a politically controversial process (see box 1).

Financial institutions and other obliged entities should be aware that a country blacklist resulting from political negotiations is necessarily biased and may not represent the full picture. Any EU list or similar lists, such as the Financial Action Task Force's (FATF) list, should be complemented by a company-specific country risk assessment, based on their countries of operations, and reliable expert and media reports about relevant AML deficiencies. This is also true for possible associations with tax havens, which appear on a separate selective EU list.

This article discusses some other modifications contained in the 5AMLD, which entails notable consequences for the practice of risk-based customer due diligence (CDD).

Centralised ownership information

The 5AMLD entails regulatory improvements for advancing the basic step of any CDD, namely the establishment of the beneficial owner of a relevant entity. The EU member states' beneficial ownership registries will be more centralised, extended and more accessible for the public in the future. This means that the registries shall be interconnected via the envisioned European Central Platform by March 2021, and there will then be an obligation to consult this platform before entering in a new business relationship. Trusts and similar arrangements will be included in the beneficial ownership registries' common platform. Unlike the current practice in some member states, the general public will be given access to the ownership information—with some

BOX 1

EDD measures with respect to high-risk third countries

Article 18a (Dir. 2018/843) requires EDD measures including obtaining additional information on the customer and the beneficial owners; the intended nature of the business relationship; the source of funds and wealth; and the reasons for the intended or performed transactions.

One particular precautionary measure may require that the "first payment be carried out through an account in the customer's name, with a credit institution subject to customer due diligence standards that are not less robust than those laid down in this directive."

In addition to increased relationship monitoring and mitigating measures on transactions with high-risk countries, the regulation suggests limitations of the business relationships, such as "refusing the establishment of subsidiaries, branches or representative offices of companies from a high-risk third country," and "prohibiting the establishment subsidiaries, branches or representative offices in a country concerned."

Another clause stipulates that "correspondent relationships with respondent institutions in a high-risk country should be reviewed and if necessary terminated."

BOX 2

Controversial list of high-risk third countries

Based on Article 9 (2) of Directive 2018/843, on the 13 of February of 2019, the European Commission presented a list of 23 high-risk third countries, which had been assessed as having strategic AML/CTF deficiencies.[4] The list went beyond the FATF list of "high-risk and monitored jurisdictions" and included 11 additional jurisdictions, among them Saudi Arabia, Panama and three U.S. territories: Puerto Rico, American Samoa and U.S. Virgin Islands. The U.S. Treasury was critical of the list.[5] At the same time, the list also drew criticism for omitting a number of countries considered to be strong candidates.[6] More importantly, the list was not supported by the European Council, which raised its veto on the 5 of March of 2019.[7] Officially the council objected for methodological reasons, although the commission explained in its proposal—C(2019)1326—why it had selected each country, and it had apparently also consulted the affected countries before including them on the list.[8]

The quarrels over the list of high-risk countries are opposite to the original idea of pursuing a harmonised approach toward high-risk countries with a focus on standard EDD and mitigant measures where applicable. In any case, the commission is reconsidering the list and will have to reach the consent of both the European Council and the European Parliament at an early stage at the risk of ending up with a watered-down list, which would harm the credibility of the whole process.

On 12 of March of 2019, the EU finance ministers adopted a revised list of countries considered to be tax havens including American Samoa, Bahrain, Aruba, Barbados, Belize, Bermuda, Dominica, Fiji, Guam, Marshall Islands, Oman, Samoa, Trinidad and Tobago, the U.S. Virgin Islands, United Arab Emirates and Vanuatu.[9] Questions remain if this list can be considered complete and meaningful, or cut short for political reasons. Of course, the list gracefully omits EU member states considered to be problematic tax jurisdictions.

restrictions regarding trusts—essentially allowing greater scrutiny by the press and civil society organisations.

Should the EU manage to effectively implement a centralised database platform containing reliable ownership information, the effect may extend well beyond the improved efficiency of know your customer (KYC) research, essentially carrying the message that any country that does not provide access to such ownership information should be regarded as a high-risk country from a regulatory perspective. In practical terms, this would imply that KYC research, which encounters barriers when establishing beneficial ownership information from public registries, could trigger risk-based EDD measures or even the next level of integrity due diligence (IDD), including an in-depth country investigation.

The fight against money laundering engages in strategic interaction, where tightening the regulation means that potential perpetrators will likely become more inventive instead of giving up. This means that an ultimate beneficial owner (UBO) who wants to stay in the hiding will either use jurisdictions that do not provide ownership information, or will hide behind layered and complex shareholding structures. In any case, intransparent structures where it is not possible to identify the UBO will further increase the risk exposure in the future.

Transparency of funds

Furthermore, 5AMLD, in a new Article 10 (1), requires member states to prohibit their credit institutions and financial institutions from keeping anonymous accounts, passbooks or safe-deposit boxes, rendering their owners and beneficiaries subject to CDD measures (in force since 10 January 2019). Furthermore, a centralised automated mechanism will be set up to allow the identification of bank and payment account holders and safe-deposit boxes

by September 2020. The information will be available for financial intelligence units and national authorities.

In practice, abolishing anonymous accounts will support establishing the source of funds of a customer. When entering a business relationship, the source of funds should always be clear. With respect to third countries, where it is not possible due to anonymity or other barriers to understand where the money came from, such high-risk factors should trigger EDD, essentially widening the scope to question the source of wealth of the customer as a whole.

From a practical perspective, in order to detect if funds come from illicit proceeds and/or are transferred as part of an ultimately illegal money laundering scheme, the flow of funds must be assessed in the context of the nature of the business relationship and the purpose of the transaction. Any suspicion that a transaction involves intermediaries—behind which ultimate owners of potentially illegitimate funds may hide—is a red flag and should trigger EDD or IDD.

Politically exposed persons

Another area where 5AMLD introduces some improvements for CDD relates to the identification of politically exposed persons (PEPs). Member states are required to develop a list of specific functions or offices (not names) that qualify as prominent public functions in the respective country, including those of registered international organisations. To what extent these lists will display differences in the classification of PEPs—for example, with respect to party leaders or mayors of larger cities—remains to be seen. In any case, the identification of a PEP, a relative or close associate of a PEP linked to any one customer relationship should be part of simplified due diligence procedure in order to trigger EDD measures should this high-risk criterion apply.

Relying on prepared PEP lists is a necessary starting point but may not be sufficient as indirect but crucial links to PEPs through associates may not be uncovered. Again, given that more and more actual PEPs will know that they are on the radar screen, those who have something to hide will try to use intermediaries in an attempt to avoid triggering a red flag.

EDD on an identified PEP comprises obtaining additional information on whether the high-risk qualification can be substantiated—for example, by proof of relevant business interests, any questionable use of power, links to irregularities or even corrupt practices—which increase the likelihood of involvement in money laundering activities. The PEP definition is a functional definition that needs to be considered in the context of the specific jurisdiction and business relationship. The threshold for defining a person with a political function as a PEP should be set lower rather than higher in order to be able to exercise the appropriate due diligence to detect corruption and money laundering when it exists.

Conclusion

The 5AMLD further raises the benchmarks for the practice of EDD on high-risk customers. Whilst the EU is struggling with political difficulties in defining high-risk jurisdictions both for money laundering/terrorist financing and tax purposes, the controversial discussion about the relevant country lists has provided financial institutions and other obliged companies with ample information about notorious countries of concern—hard to ignore when conducting due diligence on customers linked to these countries. With respect to verifying customer information, the 5AMLD carries the message that accepting a business relationship without knowing the ultimate beneficial owner and without knowing the source of funds entails serious risks of being associated with criminals and their illegal proceeds. EDD should reckon with layered ownership structures and intermediaries involved in the flow of funds. Similarly, the identification of a PEP's hidden involvement in ownership and transactions requires in-depth knowledge of a customer's political and business environment.

Dr. Carsten Giersch, senior partner, Berlin Risk Ltd., Berlin, Germany, carsten.giersch@berlinrisk.com

[1] "Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU," EUR-Lex, 30 May 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843

[2] "Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC," EUR-Lex, 20 May 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849

[3] "EU Policy on High-Risk Third Countries," European Commission, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/anti-money-laundering-and-counter-terrorist-financing/eu-policy-high-risk-third-countries_en; "EU Methodology for Identifying High-Risk Third Countries," Global Risk Affairs, 11 July 2018, https://www.globalriskaffairs.com/2018/07/eu-methodology-for-identifying-high-risk-third-countries/

[4] "Commission Delegated Regulation (EU) of 13.2.2019 supplementing Directive (EU) 2015/840 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies," European Commission, 13 February 2019, https://ec.europa.eu/info/sites/info/files/commission-delegated-regulation_hrtc.pdf

[5] "Treasury Statement on European Commission List of Jurisdictions with Strategic AML/CFT Deficiencies," U.S. Department of the Treasury, 13 February 2019, https://home.treasury.gov/news/press-releases/sm610

[6] Simon Bowers, "European Commission shames Saudi Arabia, Panama with 'dirty money' blacklist," *International Consortium of Investigative Journalists,* 14 February 2019, https://www.icij.org/blog/2019/02/european-commission-shames-saudi-arabia-panama-with-money-laundering-and-terror-financing-blacklist-but-attracts-criticism/

[7] Council of the European Union, 6964/1/19 REV 1; Bjarke Smith-Meyer, "EU countries revolt against Commission's dirty money list," *Politico*, 4 March 2019, https://www.politico.eu/article/eu-countries-revolt-against-commission-dirty-money-list-vera-jourova/

[8] "Anti-money laundering: Q & A on the EU list of high-risk third countries," European Commission, 13 February 2019, http://europa.eu/rapid/press-release_MEMO-19-782_en.htm

[9] Bjarke Smith-Meyer, "EU adopts tax haven blacklist," *Politico*, 12 March 2019, https://www.politico.eu/article/eu-adopts-tax-haven-blacklist-despite-romanian-doubts/

Fight Financial Crime with AI

Bring the power of machine learning and RPA to AML

Visit us at ACAMS Conference Berlin at Booth #31

Learn more
sas.com/acams-berlin-2019

sas
THE POWER TO KNOW®

Celebrating the ACAMS® CYPRUS CHAPTER

The ACAMS Cyprus Chapter recently celebrated its third birthday at a great venue in Nicosia! The special networking event hosted a number of members, regulators, law enforcement, as well as friends and supporters of the chapter.

The chapter was formed in November 2015 by a group of anti-money laundering (AML) and compliance enthusiasts with the support of ACAMS. The aim was to provide a platform for AML and compliance professionals in Cyprus to network, exchange ideas and enhance their knowledge. At the time, Cyprus was in the spotlight concerning the effectiveness of its AML regulatory framework and the CAMS qualification was not widely known on the island. After three years, the CAMS qualification has become recognised as the gold standard in AML certifications amongst compliance professionals, employers and recruiters in Cyprus. It now serves as proof of someone's deep knowledge and expertise in practical AML. Accordingly, every year a number of anti-financial crime (AFC) professionals register to obtain their certification.

The ACAMS Cyprus Chapter board is comprised of experienced AFC practitioners and AML compliance trainers who enjoy voluntarily organising learning and networking events for the members of the chapter and the wider AFC community of Cyprus. Dellas is the founding member and chair of the ACAMS Cyprus Chapter since its launch in 2015. Gregory Dellas was also June 2017's *ACAMS AML Professional of the Month*. He currently works in the first line of defence as the director of wealth and markets for the Bank of Cyprus. With extensive experience in AML compliance—having been CAMS certified and as a certified CAMS instructor—Dellas understands the importance of continuous learning in order to practically, efficiently and effectively combat financial crime. Dellas said the following of the Cyprus Chapter:

> "The ACAMS Cyprus Chapter is one of a kind in Cyprus. It is unique in that it offers free exciting learning and networking events to its members, multiple times a year. The events touch upon all current and future concerns of today's AML professionals and compliance enthusiasts and the events are also open to the wider community to register and attend. Our events have attracted participants from Cyprus and beyond, including regulators and law enforcement. During the last few years, Cyprus underwent a huge transformation regarding the implementation of an enhanced AML regulatory framework. We want to believe that we also played our part, through our activities."

Now entering its fourth year, the ACAMS Cyprus Chapter can proudly look back at the long list of successful events it has hosted on topics such as countering terrorist financing, correspondent banking, cybercrime, cryptocurrency and blockchain, international sanctions, politically exposed persons and their associates, General Data Protection Regulation and AML and many more. ACAMS Cyprus Chapter events have attracted a number of international speakers and experts who are willing to share their thoughts and expertise with the participants. The events always attract more than 100 AFC professionals from various industries, as well as representatives from a number of regulatory bodies.

At the latest event in early February 2019, ahead of the Anti-Financial Symposium—Cyprus, the Cyprus Chapter was proud to welcome international expert Samantha Sheen, founder and managing director of Ex Ante Advisory Limited. Sheen discussed the vulnerabilities of international financial centres around the world using the case of 1MDB as a practical example. She discussed the misuse of complex structures, financial crime through complex webs of transactions and provided valuable advice to compliance professionals in order to avoid such mistakes in the future.

In March 2019, the Cyprus Chapter organised yet another exciting event on risk-based due diligence and transaction monitoring with Jamilia Parry, managing director of FTI Consulting. The event was attended by over 120 compliance professionals from Cyprus and overseas. A number of more exciting events are also in the works.

Gregory Dellas, CAMS, director wealth & markets, Bank of Cyprus, chair of the ACAMS Cyprus Chapter, Nicosia, Cyprus, cypruschapter@acams.org

Prost to the ACAMS Germany Chapter

The Association of Certified Anti-Money Laundering Specialists (ACAMS) launched its Germany Chapter in late 2016. Since then, the chapter has hosted approximately 20 events across the country at its main hubs in Berlin, Frankfurt and Munich. The networking events, which draw between 50 to 100 participants, have covered a wide range of topics including upcoming regulatory challenges, and specific challenges related to know your customer, transaction monitoring, sanctions risks, terrorist financing and human trafficking. Other interesting sessions have discussed the changing role of the anti-financial crime (AFC) function and that of the AFC professional within the context of digitization and emerging technology. Within this context, a number of events were held to discuss other emerging topics such as regtech, fintech, virtual currencies, cybercrime and trade-based money laundering.

Germany Chapter speakers have included experts from the following traditional financial institutions: Allianz, Commerzbank, Deutsche Bank, figo, HSBC, KfW, UBS, UniCredit and Western Union. Fintech company speakers have come from Bitwala, Circle, Coinfirm, figo, Fidor Bank, N26 and solarisBank. In addition, there have been representatives from non-financial institutions including AirPlus International, MAN Group and Scout24. From the public sector, representatives involved in the legislative process and enforcement from the German Federal Ministry of Finance and the Federal Police Inspectorate have also engaged in discussions. Consulting firm members from Berlin Risk, Deloitte, EY, Huxley Associates, KPMG, Protiviti, PwC and solution providers from Accuity, Alyne, Bureau van Dijk, Dow Jones, FinScan, LexisNexis Risk Solutions, Oracle and SAS have not only contributed their knowledge and shared best practice standards, but have also sponsored and facilitated the networking events across the industry.

Besides generating a platform for networking and exchanging best practices, the ACAMS Germany Chapter has launched two working groups: one in Berlin that looks at fintech topics and another in Frankfurt that addresses AFC audit. The working groups provide a platform of exchange on common challenges related to regulatory and operational topics.

For a more in-depth overview of events, membership details and information about upcoming events, please visit the chapter page at http://www.acams.org/acams-chapters/germany. The ACAMS Germany Chapter is keen to expand its membership in Germany and engage with interested sponsors for future chapter events. If you are interested in joining the community, please email germanychapter@acams.org.

Jennifer Hanley-Giersch, CAMS, CFE, board member of the ACAMS Germany Chapter, managing partner, Berlin Risk Ltd., Berlin, Germany, jennifer.hanley@berlinrisk.com


COUNTER
EXTREMISM
PROJECT
CURRENT CHALLENGES IN COUNTERING TERRORISM FINANCING
ACAMS GERMAN CHAPTER EVENT
BERLIN 28.03.19


Thank you


Will Technology
Save Us?


Terrorism Financing

Handelsbasierte Geldwäsche–
Risikofaktoren und Sorgfaltspflichten

Das seit dem 30. November 1993 in Deutschland geltende Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz—GwG) wurde zum 21. August 2008 neu gefasst und später durch das Gesetz zur Optimierung der Geldwäscheprävention (Geldwäscheoptimierungsgesetz—GwOptG) geändert, welches am 29. Dezember 2011 bzw. 31. März 2012 in Kraft trat. Am 26. Juni 2017 wurde das Geldwäschegesetz mit dem Gesetz zur Umsetzung der Vierten EU-Geldwäscherichtlinie erneut revidiert und neu gefasst. Die 5. EU-Geldwäscherichtlinie (Richtlinie (EU) 2018/843) zur Änderung der 4. EU-Geldwäscherichtlinie trat am 9. Juli 2018 in Kraft. Die EU-Mitgliedstaaten müssen die Richtlinie bis zum 10. Januar 2020 in nationales Recht umsetzen.

Nach dem deutschen Geldwäschegesetz zählen bereits seit 2012 auch Güterhändler zu den Verpflichteten (§ 2 Abs. 1 GwG).[1] Der Begriff des Güterhändlers, der in § 1 Abs. 9 GwG definiert wird, umfasst einen weiten Personenkreis und meint „jede Person, die gewerblich Güter veräußert, unabhängig davon, in wessen Namen oder auf wessen Rechnung sie handelt".[2] Mit Gütern im Sinne des Geldwäschegesetzes sind alle beweglichen und nicht beweglichen Sachen (mithin auch Grundstücke und sonstige Immobilien) gemeint, „unabhängig von ihrem Aggregatzustand, die einen wirtschaftlichen Wert haben und deshalb Gegenstand einer Transaktion sein können".

Ein Verdachtsfall liegt laut Gesetz vor, wenn Tatsachen darauf hindeuten, dass ein Vermögensgegenstand aus einer Vortat der Geldwäsche stammt oder im Zusammenhang mit Terrorismusfinanzierung steht. Nach Auffassung der Behörden besteht die Meldepflicht, sobald bekannte Anhaltspunkte für Geldwäsche bzw. Terrorismusfinanzierung vorliegen oder sich bestehende Zweifel trotz versuchter Aufklärung nicht ausräumen lassen. Das Vorliegen einzelner *Red Flags* (siehe Tabelle: Risikofaktoren) muss dabei nicht automatisch zu einer Meldepflicht führen, kann aber, abhängig von den sonstigen Umständen, auf einen Verdachtsfall hinweisen und sollte demzufolge weitere Prüfschritte auslösen. Eindeutig ist die Meldepflicht allerdings bei der Verletzung von Mitwirkungspflichten. Kommt der Geschäftspartner seiner Pflicht zur Offenlegung, ob er für einen wirtschaftlich Berechtigten handelt, nicht nach, muss auf jeden Fall eine Verdachtsmeldung gemacht werden.

Der folgende Artikel befasst sich mit den Anforderungen im Bereich der Geschäftspartnerprüfung sowie einer Reihe von Risikoindikatoren für die handelsbasierte Geldwäsche.

Risikoanalyse

Bei der Bekämpfung von Geldwäsche und Terrorismusfinanzierung steht an erster Stelle die Wahrnehmung der Sorgfaltspflichten.[3] Hierbei wird nach allgemeinen, vereinfachten und verstärkten Sorgfaltspflichten unterschieden. Können bestimmte Sorgfaltspflichten nicht erfüllt werden, darf eine Geschäftsbeziehung nicht begründet oder fortgesetzt werden. Es dürfen keine Transaktionen durchgeführt werden, bereits bestehende Geschäftsbeziehungen sind zu beenden.

Verpflichtete müssen nur vereinfachte Sorgfaltspflichten erfüllen, soweit sie unter Berücksichtigung der Risikofaktoren (siehe Tabelle: Risikofaktoren) feststellen, dass in bestimmten Bereichen, insbesondere im Hinblick auf Kunden, Transaktionen und Dienstleistungen oder Produkte, nur ein geringes Risiko der Geldwäsche oder der Terrorismusfinanzierung besteht.

Für Güterhändler gelten erleichterte Pflichten. Die allgemeinen kundenbezogenen Kernsorgfaltspflichten müssen Güterhändler immer nur dann beachten, wenn sie Geschäfte mit Bargeldtransaktionen im Wert von über 10.000 Euro tätigen—bei gestückelten Zahlungen gilt der Gesamtbetrag—oder einen begründeten Verdacht auf Begehung einer Geldwäschestraftat nach § 261 Strafgesetzbuch (StGB) oder der Terrorismusfinanzierung (unabhängig von der Höhe der Transaktion) haben.

Sorgfaltspflichten (Geschäftspartnerprüfung / KYC)

Zu den allgemeinen Sorgfaltspflichten (auch Geschäftspartnerprüfung / KYC genannt), welche die betreffenden Unternehmen gegenüber ihren Geschäftspartnern gegebenenfalls anzuwenden haben, gehören folgende Schritte: die Identifizierung des Vertragspartners, die Einholung von Informationen über die Art und den Zweck der Geschäftsbeziehung, die Abklärung, ob der Vertragspartner für einen wirtschaftlich Berechtigten (d.h. die natürliche Person, die letztlich den Auftrag zu einer Transaktion gibt) handelt, und, falls dies der Fall ist, dessen Identifizierung sowie die kontinuierliche Überwachung der Geschäftsbeziehung einschließlich der im Verlauf durchgeführten Transaktionen.

Soweit erhöhte Risiken von Geldwäsche und Terrorismusfinanzierung vorliegen, haben Unternehmen zusätzliche, dem erhöhten Risiko angemessen verstärkte Sorgfaltspflichten zu erfüllen. Verstärkte Sorgfaltspflichten sind aber nur dann zu beachten, wenn bereits allgemeine Sorgfaltspflichten bestehen. Das bedeutet für Güterhändler, dass auch die verstärkten Sorgfaltspflichten nur im Verdachtsfall oder bei Bargeldtransaktionen im Wert von über 10.000 Euro greifen.

Zu Vertragspartnern (einschließlich eventuell vorhandener wirtschaftlich Berechtigter) mit erhöhtem Risiko zählen dabei vor allem Politisch Exponierte Personen (PEPs). Im weitesten Sinne umfasst dieser Begriff alle Menschen, denen eine wichtige öffentliche Position in einem bestimmten Land anvertraut ist oder war. Die juristische Definition der PEPs ist, ebenso wie die Definition von Korruption, von Land zu Land verschieden. Zu dieser Gruppe gehören z.B. Staatsoberhäupter oder Regierungschefs, Kabinettsmitglieder und Politiker in anderen leitenden Funktionen, Amtsträger bei Gerichten oder beim Militär,

Tabelle: Risikofaktoren

FAKTOREN FÜR EIN POTENZIELL GERINGERES RISIKO	FAKTOREN FÜR EIN POTENZIELL HÖHERES RISIKO
Kundenrisiken	
• öffentliche, an einer Börse notierte Unternehmen, die aufgrund von Börsenordnungen oder gesetzlicher Regelungen Offenlegungspflichten unterliegen, was die Gewährleistung einer angemessenen Transparenz hinsichtlich des wirtschaftlichen Eigentümers betrifft • öffentliche Verwaltungen oder Unternehmen • Kunden mit Wohnsitz in geografischen Gebieten mit geringerem Risiko (s.u.)	• außergewöhnliche Umstände der Geschäftsbeziehung • Kunden, die in geografischen Gebieten mit hohem Risiko ansässig sind (s.u.) • juristische Personen oder Rechtsvereinbarungen, die als Instrumente für die private Vermögensverwaltung dienen • Unternehmen mit nominellen Anteilseignern oder mit als Inhaberpapieren emittierten Aktien • bargeldintensive Unternehmen • eine angesichts der Art der Geschäftstätigkeit als ungewöhnlich oder übermäßig kompliziert erscheinende Eigentumsstruktur des Unternehmens
Produkt-, Dienstleistungs-, Transaktions- oder Vertriebskanalrisiken	
• Lebensversicherungspolicen mit niedriger Prämie • Versicherungspolicen für Rentenversicherungsverträge, sofern die Verträge weder eine Rückkaufklausel enthalten noch als Sicherheit für Darlehen dienen können • Rentensysteme und Pensionspläne oder vegleichbare Systeme, die den Arbeitnehmern Altersversorgungsleistungen bieten, wobei die Beiträge vom Gehalt abgezogen werden und die Regeln des Systems den Begünstigten nicht gestatten, ihre Rechte zu übertragen • Finanzprodukte oder -dienste, die bestimmten Kunden angemessen definierte und begrenzte Dienstleistungen mit dem Ziel der Einbindung in das Finanzsystem („financial inclusion“) anbieten • Produkte, bei denen die Risiken der Geldwäsche und der Terrorismusfinanzierung durch andere Faktoren wie etwa Beschränkungen der elektronischen Geldbörse oder die Transparenz der Eigentumsverhältnisse verringert werden (z.B. bei bestimmten Arten von E-Geld)	• Betreuung vermögender Privatkunden • Produkte oder Transaktionen, die Anonymität begünstigen könnten • Geschäftsbeziehungen oder Transaktionen ohne persönliche Kontakte und ohne bestimmte Sicherungsmaßnahmen wie z.B. elektronische Unterschriften • Eingang von Zahlungen unbekannter oder nicht verbundener Dritter • neue Produkte und neue Geschäftsmodelle einschließlich neuer Vertriebsmechanismen sowie Nutzung neuer oder in der Entwicklung begriffener Technologien für neue oder bereits bestehende Produkte
Geografisches Risiko	
• EU-Mitgliedstaaten • Drittstaaten mit gut funktionierenden Systemen zur Verhinderung, Aufdeckung und Bekämpfung von Geldwäsche und von Terrorismusfinanzierung • Drittstaaten, in denen Korruption und andere kriminelle Tätigkeiten laut glaubwürdigen Quellen schwach ausgeprägt sind • Drittstaaten, deren Anforderungen an die Verhinderung, Aufdeckung und Bekämpfung von Geldwäsche und von Terrorismusfinanzierung laut glaubwürdigen Quellen (z.B. gegenseitige Evaluierungen, detaillierte Bewertungsberichte oder veröffentlichte Follow-up-Berichte) den überarbeiteten Empfehlungen der FATF (Financial Action Task Force) entsprechen und die diese Anforderungen wirksam umsetzen	• unbeschadet des Artikels 9 der Richtlinie (EU) 2015/849 ermittelte Länder, deren Finanzsysteme laut glaubwürdigen Quellen (z.B. gegenseitige Evaluierungen, detaillierte Bewertungsberichte oder veröffentlichte Follow-up-Berichte) nicht über hinreichende Systeme zur Verhinderung, Aufdeckung und Bekämpfung von Geldwäsche und Terrorismusfinanzierung verfügen • Drittstaaten, in denen Korruption oder andere kriminelle Tätigkeiten laut glaubwürdigen Quellen signifikant stark ausgeprägt sind • Staaten, gegen die beispielsweise die Europäische Union oder die Vereinten Nationen Sanktionen, Embargos oder ähnliche Maßnahmen verhängt haben • Staaten, die terroristische Aktivitäten finanziell oder anderweitig unterstützen oder in denen bekannte terroristische Organisationen aktiv sind

leitende Angestellte bei staatlichen Unternehmen sowie wichtige Vertreter der politischen Parteien. Da PEPs ständig im Licht der Öffentlichkeit stehen, engagieren sie häufig Mittler und Zwischenhändler, um in ihrem Auftrag finanzielle Transaktionen oder damit im Zusammenhang stehende Aktivitäten durchzuführen. Als Mittelsleute von PEPs können enge Vertraute, Geschäftspartner oder Freunde und Familienmitglieder dienen. Sofern ein hohes Risiko identifiziert wurde, sind vor allem folgende Maßnahmen zu ergreifen:

- die Begründung oder Fortführung einer Geschäftsbeziehung bedarf der Zustimmung eines Mitglieds der Führungsebene,
- es sind angemessene Maßnahmen zu ergreifen, mit denen die Herkunft der Vermögenswerte bestimmt werden kann, die im Rahmen der Geschäftsbeziehung oder der Transaktion eingesetzt werden,
- und die Geschäftsbeziehung ist einer verstärkten kontinuierlichen Überwachung zu unterziehen.

Seit der 5. EU-Geldwäscherichtlinie gilt der sogenannte „erweiterte risikobasierte Ansatz" in Bezug auf die Sorgfaltspflichten. Angestrebt wird ein strukturierter und methodischer Ansatz, der durch entsprechende Feinabstimmung von Prüfungsumfang und Untersuchungstiefe zu sinnvollen Ergebnissen führt. Dabei kann die Methodik, die der Auswertung der Recherche und der Erstellung individueller Risikoprofile zugrunde liegt, auf einen einzelnen Fall ebenso wie auf standardisierte Verfahren hin angepasst werden. Eine zentrale Rolle spielt die Ermittlung von Red Flags, welche die Reputation eines Geschäftspartners oder Unternehmens in Frage stellen.

Typologien der Handelsbasierten Geldwäsche—an der Schnittstelle zwischen Unternehmen und Finanzinstitute

Der FATF-Typologie-Bericht (siehe unten) nennt einige grundlegende Techniken, die bei handelsbasierter Geldwäsche eingesetzt werden:

- die Ausstellung von Rechnungen mit zu geringen oder zu hohen Preisen für Lieferungen und Leistungen
- Mehrfachabrechnungen von Lieferungen und Leistungen
- Lieferungen und Leistungen mit zu wenig oder zu viel Inhalt
- Falschbeschreibungen von Lieferungen und Leistungen

Eine der häufigsten Methoden, um in betrügerischer Weise Werte über nationale Grenzen zu bringen, ist die Ausstellung von Rechnungen mit zu geringen oder zu hohen Preisen für Lieferungen und Leistungen. Sehr häufig ist die Falschangabe des Preises mit dem Ziel, zwischen Importeur und Exporteur einen Mehrwert zu übertragen. Dieser Kanal ist u.a. deshalb so lukrativ, weil es für die Zollbehörden oft schwierig ist, handelsbasierte Geldwäsche als solche zu identifizieren, insbesondere wenn die Preisstrukturen unklar und die Märkte undurchsichtig sind (z.B. bei Kunst, Antiquitäten oder dem Handel mit Gebrauchtwagen).

Durch den wachsenden internationalen Handel und die damit verbundenen langen Lieferketten ist das Handelsgeschäft besonders anfällig für Geldwäsche, Korruption, Betrug und Steuerhinterziehung. Dabei stellen die zuletzt genannten Delikte häufig Vortaten zur handelsbasierten Geldwäsche dar. Im Jahr 2012 hat die Asia Pacific Group der FATF den *APF Typology Report on Trade Based Money Laundering* veröffentlicht. Dort wurden die folgenden Haupttypen für Geldwäsche bei der Finanzierung im Handelsgeschäft dargestellt:

- **Mittelzuflussbasierte Zahlungen** *(Cash Inflow Based Payment)*—Zahlungen werden ‚strukturiert' oder über sogenannte ‚Smurfing'-Techniken (abgeleitet von „Smurfs", dem englischen Namen der Schlümpfe) in den Finanzkreislauf integriert, um Handelstransaktionen abzuwickeln. Die Bezahlung erfolgt bar in zumeist zahlreichen kleinen Tranchen.
- **Zahlungen an Drittparteien** *(Third Party Payment)*—Drittparteien werden als Mittler zwischen Händlern aus zwei unterschiedlichen Ländern eingeschaltet, um den Handelsfinanzierungsvertrag zu unterstützen oder bei Factoring oder Forfaitierung mitzuwirken.
- **Segmentierte Zahlungsweisen** (*Segmental Modes of Payment)*—mit diesem System werden mehrere Handelsfinanzierungen herbeigeführt, um eine Transaktion zu finanzieren. Dieses System wird öfters eingesetzt, wenn eine Drittpartei zwischen Exporteur und Importeur geschaltet wird. Für den Import können Akkreditiv-Instrumente eingesetzt und für den Reexport dann Banküberweisungen genutzt werden.
- **Alternative Überweisungsmodalitäten** *(Alternative Remittance Payment)*—Handelstransaktionen, die für handelsbasierte Geldwäsche anfällig sind, können den Transfer von Gütern beinhalten, deren richtiger Wert nicht mit dem Betrag übereinstimmt, der offiziell bezahlt wird. Um diese Spanne zu finanzieren, werden alternative Zahlungsmodalitäten eingesetzt. Der Abgleich der Differenz erfolgt gewöhnlich durch

Tabelle: Risikofaktoren

Risikobereiche	Red Flags
Kundenrisiken	
Handelsfinanzierung	• Barzahlungen, Überweisungen oder sonstige Zahlungen von unabhängigen Drittparteien oder Intermediären, die keine unmittelbare Beziehung zu dem Verkäufer oder Käufer unterhalten • Akkreditive, die öfters geändert oder erweitert worden sind, ohne dass sich der Berechtigte oder der Ort des Zahlungsvorgangs ändert, oder auch für Aktivitäten, die mit dem Kerngeschäft nichts zu tun haben • Unfähigkeit des Kunden, eine angemessene Dokumentation für eine Transaktion vorzuweisen • Zahlungen, die inkonsistent mit den Risikoeigenschaften der Transaktion sind, z.B. Vorauszahlung für eine Lieferung von einem neuen Zulieferer aus einem hochriskanten Land oder häufige Transaktionen, wobei die Beträge runde Zahlen darstellen • sogenanntes *Phantom Shipping,* wobei keine Güter verschifft werden und jegliche Dokumentation gefälscht ist • handelbare Wertpapiere, Reiseschecks oder Zahlungsanweisungen • Zahlungen von verschiedenen Konten auf mehrere Konten der Gegenseite • unterschiedliche Finanzierungsmechanismen für die Importseite und die Exportseite einer handelsgeschäftlichen Transaktion
Länder	• Transaktionen in oder von Hochrisikoländern • ein Hochrisikoland dient als Umschlagplatz ohne erklärbaren kommerziellen Grund • Aktivitäten in Freihandelszonen wegen der dortigen begrenzten Zollkontrollen • Versand über einen nicht zu erklärenden Umweg oder Versand von Gütern über eine Route, die von den normalen Handelsrouten abweicht (z.B. werden Halbleiterprodukte in Länder exportiert, die keine elektronische Industrie haben)
Produkte	• signifikante Abweichungen zwischen Beschreibung, Qualität, Quantität oder Wert der Waren auf Dokumenten wie Rechnungen, Konnossementen und den tatsächlich verschifften Waren • Fehldarstellung der Art der Waren oder deren Qualität • Umfang der Sendung ist inkonsistent mit der Größe des Geschäfts des Exporteurs oder Importeurs oder übersteigt dessen Kapazität • die Sendung bzw. Investition ergibt ökonomisch keinen Sinn
Unternehmensstrukturen	• Vorratsgesellschaften oder Briefkastenfirmen • große Zahl von Einzelpersonen und Gesellschaften oder Gesellschaften mit beschränkter Haftung gegründet von unabhängigen Drittparteien • Verwendung von Stimmrechtsvertretern, eventuell unter Nutzung gefälschter Adressen • Transaktionen zwischen geschäftlich verbundenen Parteien wie beim Umsatzsteuer-Karussell

Ausgleichszahlungen in Landeswährung an Personen vor Ort, die als designierte Partner des im Ausland angesiedelten Handelspartners fungieren.

Der Bericht enthält ferner eine Liste von Red Flags, die im Zusammenhang mit Handelsfinanzierung und handelsbasierter Geldwäsche zu beachten sind.

Zusammenfassung

Die 5. EU-Geldwäscherichtlinie verpflichtet Unternehmen dazu, vermehrt risiko-fokussiert zu agieren, was die Geschäftspartnerprüfung angeht. Das bezieht sich nicht nur auf die Entscheidung, ob vereinfachte oder verstärkte Sorgfaltspflichten gelten, sondern auch darauf, welche Methoden, Quellen und Monitoring-Ansätze angebracht sind.

Anhand definierter Red Flags können Kriterien maßgeschneidert für Sektoren, Länder, Kunden und Projekte entwickelt werden. Somit sind die Unternehmen in der Lage, ihre Verfahren so auszurichten, dass den erweiterten risikobasierten Anforderungen Genüge getan und im Sinne eines soliden Risikomanagements die eigene Reputation geschützt wird. In Zukunft werden die Unternehmen moderne Methoden der Risikoanalyse und Risikobewertung einsetzen müssen, um die gestiegenen Herausforderungen im Bereich der Geldwäscheprävention zu meistern.

Jennifer Hanley-Giersch, CAMS, CFE, managing partner, Berlin Risk Ltd., Berlin, Germany, jennifer.hanley@berlinrisk.com

[1] "Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz - GwG)," Bundesministeriums der Justiz und für Verbraucherschutz, 23 July 2017, https://www.gesetze-im-internet.de/gwg_2017/BJNR182210017.html

[2] Ibid.

[3] "International Standards On Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations," Financial Action Task Force, October 2018, http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF Recommendations 2012.pdf

Ein Sammelsurium von Vorschriften

Blockchain-Technologie bietet eine breite Palette von Lösungen, die herkömmliche Geschäftsmodelle in Frage stellen. Diese Innovation bedarf jedoch aktualisierter Governance-Richtlinien, um die Effizienz mit der öffentlichen Sicherheit in Einklang zu bringen. Blockchain-Technologie kann autonomen Benutzern ermöglichen, Vermögen selbstständig zu überweisen—schnell, weltweit, jederzeit und ohne Zwischenhändler. Hierfür wird der bisher erfolgreichste Verwendungszweck genutzt—Kryptowährungen. Durch diese Technologie erhöhen sich Transparenz und Nachverfolgbarkeit. Typischerweise werden alle Blockchain-Transaktionen in einem Distributed Ledger (einem verteilten Kassenbuch) erfasst. Allerdings ist die Technologie auch anfällig für mit Marktmissbrauch, Geldwäsche und Terrorismusfinanzierung verbundene Risiken.

Weltweit haben Aufsichtsbehörden die in Verbindung mit Kryptowährungen neu entstehenden Risiken erkannt und verschiedene Ansätze verfolgt, um diese Risiken zu mindern und zu managen. Einige Aufsichtsbehörden definieren Kryptowährungen und Kryptowährungsdienstleister dem bestehenden aufsichtsrechtlichen Rahmen entsprechend wie herkömmliche Finanzdienstleistungsanbieter. Somit unterliegen diese auch vergleichbaren Anforderungen in Bezug auf die Geldwäsche-Prävention/Anti-Terrorismusfinanzierung (AML/CTF). Andere Aufsichtsbehörden erkennen die Wichtigkeit eines speziell für Kryptowährungen konzipierten aufsichtsrechtlichen Rahmenwerks und haben sichere Räume geschaffen, in denen diese neu entstehende Industriesparte wachsen kann.

Heute ist die Sparte in vielen Rechtssystemen nach wie vor nicht reguliert. Falls in Rechtssystemen Leitlinien angewandt werden, sind diese nicht einheitlich. Laut einem von CipherTrace im Oktober 2018 veröffentlichten Bericht flossen in der Tat „97 % der von Börsen direkt erhaltenen illegalen Bitcoins in solche, die in Ländern mit schwachen AML-Gesetzen angesiedelt sind“, und „4,7 % der von Börsen in Ländern mit schwachen Vorschriften erhaltenen Bitcoins sind illegal.”[1] Diese Statistiken basieren auf nachweislichen Fällen von Bitcoin-Überweisungen durch Verbrecher. Sie belegen den Hang von Kriminellen, Länder mit schwachen Anti-Geldwäsche- bzw. AML-Gesetzen auszunutzen. Deshalb ist es unerlässlich, einen weltweiten Standard für einen Aufsichtsrechtsrahmen zu schaffen, der den neu entstehenden Chancen ebenso wie den Risiken gerecht wird, die sich durch Kryptowährungen und deren Anbieter ergeben. Dieser Artikel bietet eine kurze Einführung in den von den Vereinigten Staaten, der Europäischen Union, der Schweiz, Großbritannien, Japan, Malta und der Financial Action Task Force (FATF) vorgeschlagenen aufsichtsrechtlichen Rahmen. Weiterhin werden die mit nicht regulierten Märkten verbundenen Risiken und der internationale Charakter dieser Risiken am Beispiel des angeblichen Geldwäsche-Falls von Alexander Vinnik untersucht.

USA

Die Vereinigten Staaten können als das erste Land angesehen werden, das Vorschriften zu Kryptowährungen in Kraft gesetzt hat. Im März 2013 gab das Financial Crimes Enforcement Network (FinCEN) Leitlinien heraus, in denen Tauschbörsen und Administratoren von Kryptowährungen als Money Transmitters definiert sind, eine Art von gemäß dem Bank Secrecy Act von 1970 (BSA) definierten Finanzdienstleistungsunternehmen (Money Service Business, MSB).[2]

Jedes laut BSA als ein MSB definierte Unternehmen ist verpflichtet, ein wirksames AML-Programm einzurichten und zu pflegen. Aufgrund dieser Definition sind große US-Kryptowährungszentren in der Lage, Geldwäsche und Terrorismusfinanzierung zu bekämpfen. Diese Entscheidung stellt einen wichtigen Richtungswechsel in der Geschichte der Kryptowährungen dar. Sie setzte weltweit ein eindeutiges Zeichen, dass innovative, zur Übertragung von Vermögen genutzte Instrumente, beispielsweise Kryptowährungen, der Aufsicht unterliegen müssen, um die Risiken der Verwendung durch skrupellose Akteure zu kontrollieren. Zudem zeigte sie, dass ein Instrument selbst nicht als Währung, Ware oder Wertpapier definiert sein musste, um der Aufsicht zu unterliegen. Diese Vorschriften waren nicht auf Definitionen ausgerichtet, sondern vielmehr auf die Bedeutung der Risiken, die durch Unternehmen entstehen, die diese Instrumente nutzen, und der Kontrollen, die von bestehenden Gesetzen betroffen sein könnten.

Um gemäß dem BSA und unter Beaufsichtigung des FinCEN tätig zu sein, müssen Tauschbörsen und Administratoren zusätzlich zur Erfüllung anderer Anforderungen AML-Richtlinien und -Verfahren entwickeln, verdächtige Transaktionen melden, Anfragen von Strafverfolgungsbehörden beantworten und Kundenidentifikationsprogramme entwickeln. Die Informationen, die von regulierten Finanzdienstleistungsunternehmen durch ihre Kundenidentifikationsprogramme und Meldungen verdächtiger Transaktionen erfasst werden, sind für Strafverfolgungs- und Aufsichtsbehörden von enormem Wert. Der Grund ist, dass Transaktions- und Einzahlungsadressen auf Blockchains lediglich als alphanumerischer Code angezeigt und diese Aktivität deshalb als anonym gesehen wird. Entsprechend den Anforderungen von Kundenidentifikationsprogrammen überprüfen Finanzdienstleistungsunternehmen die Identität und Bankkonten eines Kunden. Diese können mit der/den Einzahlungsadresse(n) des Kunden für Kryptowährungen verbunden werden. Damit wird die Datenlücke zwischen dem herkömmlichen Bankensystem und dem Kryptowährungssystem geschlossen.

Im November 2018 demonstrierte das Office of Foreign Assets Control (OFAC) die Wichtigkeit des Abgleichs identifizierbarer Informationen mit Kryptowährungsdaten (beispielsweise Einzahlungsadressen). Das OFAC veröffentlichte die Identitäten und damit verbundenen Einzahlungsadressen zweier iranischer Staatsbürger, die geholfen hatten, durch eine Ransomware-Attacke erhaltene Bitcoins in Fiatgeld zu konvertieren.[3] Diese Einzahlungsadressen können auf der Blockchain zurückverfolgt werden. Kryptowährungsdienstleister können diese Informationen nutzen, um direkte Verbindungen zwischen ihren Benutzern und den vom OFAC identifizierten Personen festzustellen.

Schweiz

Die Schweiz ging noch einen Schritt weiter als die USA. Das Land hat amtliche Bewilligungsstrukturen für Kryptowährungsanbieter eingeführt, ebenso wie zusätzliche Anforderungen zu denen, die für Finanzdienstleister gelten. Im Oktober 2018 erteilte die Schweizer Eidgenössische Finanzmarktaufsicht FINMA die weltweit erste Vermögensverwaltungslizenz an eine Kryptowährungsplattform.[4] Im Wesentlichen ist dieses Unternehmen damit befähigt, in der Schweiz wie herkömmliche Vermögensverwalter tätig zu sein. Kryptowährungsbörsen in der Schweiz können bei der FINMA Vermögensverwaltungslizenzen beantragen. Die Schweizerische Bankiervereinigung hat ebenfalls Leitlinien herausgegeben, die Banken helfen können, das Risiko virtueller Währungsanbieter zu bewerten. Das beinhaltet bestimmte Know-Your-Customer- (KYC-) und AML-Prüfungen, die Banken bei Initial Coin Offerings (ICO) durchführen. Diese Geschäftsvorgänge ähneln einem Börsengang und beinhalten die Ausgabe neuer Tokens. Die Leitlinien der Schweizerischen Bankiervereinigung können Kryptowährungsanbietern helfen, herkömmliche Bankendienste anzubieten.

Seit dem 1. Januar 2019 bietet die FINMA außerdem eine Fintech-Bewilligung an. Entsprechend zugelassene Nichtbankinstitute dürfen öffentliche Einlagen von bis zu 100 Millionen Schweizer Franken akzeptieren und Security Tokens auch ohne Einholung einer zusätzlichen Wertpapierhändlerlizenz verwahren. Diese Bewilligung ist ein weiteres Mittel für die Schweizer Aufsichtsbehörden, die Markteintrittsbarrieren für Kryptowährungsanbieter zu verringern und gleichzeitig den Sektor zu beaufsichtigen.

Im Hinblick auf die Liquiditäts-, Kredit- und Marktrisiken der Handelsaktivitäten institutioneller Investoren in Kryptowährungen scheint die FINMA einen konservativeren Ansatz zu verfolgen. So nennt sie beispielsweise eine Handelsobergrenze für Kryptowährungen von 4 Prozent des Gesamtkapitals für institutionelle Investoren und schlägt aufgrund des Kredit- und Liquiditätsrisikos sowie der Marktvolatilität eine Risikogewichtung von 800 Prozent für Kryptowährungen im oberen Bereich vor. Aktuell gibt es in der Schweiz keine Vorschriften, die sich spezifisch auf Kryptowährungen beziehen. Kryptowährungsanbieter unterliegen jedoch den geltenden AML- und Wertpapiervorschriften.

Europäische Union

Im Juni 2018 wurden Börsenplattformen für Kryptowährungen und Anbieter von Treuhand-Wallets in die Definition von Verpflichteten laut der fünften EU-Anti-Geldwäscherichtlinie (5AMLD) aufgenommen. Infolgedessen werden EU-Mitgliedstaaten Verpflichteten, die Kryptowährungsanbieter sind, ab Januar 2020 die Anwendung von AML-/CTF-Kontrollen auferlegen. Zudem müssen Mitgliedstaaten entsprechende Gesetze, Vorschriften und administrative Bestimmungen verabschiedet haben, um der Kryptowährungsindustrie gerecht zu werden.

Die Europäische Wertpapier- und Marktaufsichtsbehörde (ESMA) und die Europäische Bankenaufsichtsbehörde (EBA) haben ebenfalls Berichte zu ICOs und Kryptowährungen veröffentlicht. Beide Behörden haben Bedenken über die Anwendbarkeit aktueller EU-Gesetze auf Kryptowährungen geäußert. In beiden Berichten wird festgehalten, dass ein Großteil von Kryptowährungsaktivitäten im Rahmen aktueller EU-Vorschriften nicht geregelt ist. Das Vorgehen von Aufsichtsbehörden auf nationaler Ebene ist daher unkoordiniert und offensichtlich sehr unterschiedlich.

Als Finanzinstrumente geltende Kryptowährungen unterliegen der zweiten Richtlinie über Märkte für Finanzinstrumente (MiFID II). Die MiFID II wird auf nationaler Ebene je nach EU-Mitgliedsstaat anders ausgelegt. Beispielsweise gibt es unterschiedliche Ansätze dafür, ob MiFID-II-Verpflichtungen auf der Fondsebene oder auf die Managementgesellschaft anwendbar sind. Die MiFID II erlegt typischerweise Vorschriften für Investmentfirmen auf, die Portfolioverwaltungsdienste anbieten. In einigen EU-Ländern dürfen jedoch Investmentfirmen, die gemeinsame Portfolioverwaltungsdienste erbringen und Wertpapiervorschriften unterliegen, diese Dienste auch ohne eine Eintragung als Investmentfirma erbringen. Auch dies führt in Bezug auf die Beaufsichtigung von Kryptowährungen zu Unterschieden in verschiedenen Mitgliedstaaten. Deshalb empfehlen die ESMA und die EBA in ihren Berichten der Europäischen Kommission, aufsichtsrechtliche Standards festzulegen, um die Risikominderungsmaßnahmen zu vereinheitlichen.

Laut einer von der Statis Group durchgeführten Studie flossen 11 Prozent der 2018 vorgenommenen ICO-Finanzierungen, oder 1,34 Milliarden $ von 11,9 Milliarden $, in verschiedenen Tokens in betrügerische Aktivitäten.[5] Pincoin trug wesentlich dazu bei. Dieser Anbieter war für einen ICO-Exit-Betrug in Höhe von 660 Millionen $ verantwortlich, dem 32.000 Investoren zum Opfer fielen. Verbraucherwarnungen über die mit ICO-Investitionen verbundenen Risiken scheinen keinen ausreichenden Schutz für Investoren zu bieten. Der ESMA-Vorsitzende Steven Maijoor räumte ein, dass Verbraucher aufgrund der aktuell mangelnden Beaufsichtigung von Kryptowährungen einem erheblichen Betrugsrisiko durch ICOs ausgesetzt sind. Am 9. Januar 2019 gab die ESMA einen Bericht über ICOs und virtuelle Währungen heraus. Darin wird empfohlen, dass bestimmte virtuelle Währungen, die die Kriterien als Finanzinstrumente oder elektronisches Geld nicht erfüllen, spezifischen, auf ihre einzigartigen Risiken hin ausgerichteten Vorschriften unterliegen sollten.

Vereinigtes Königreich

In Großbritannien wurde der Sanctions and Anti-Money Laundering Act 2018 verabschiedet. Demnach kann das Land nach Verlassen der EU eigene AML-/CTF-Vorschriften einführen. Wahrscheinlich wird das Vereinigte Königreich die 5AMLD als Mindeststandard übernehmen. Der für die Richtlinie festgelegte spätmöglichste Umsetzungstermin liegt noch vor dem britischen EU-Austritt.

Die im März 2018 gegründete Cryptoassets Taskforce setzt sich aus Vertretern des britischen Finanz- und Wirtschaftsministeriums, der Financial Conduct Authority und der Bank of England zusammen und veröffentlichte vor Kurzem ihren Abschlussbericht, in dem drei verschiedene Arten von Kryptowährungen definiert sind: Exchange Tokens, Security Tokens und Utility Tokens. Über Blockchain-Technologie genutzte Exchange Tokens werden nicht von einer zentralen Stelle ausgegeben oder garantiert und werden als Tauschmittel verwendet (beispielsweise Bitcoin). Security Tokens sind bestimmte, benannte Investments, übertragbare Wertpapiere oder Finanzinstrumente, denen Rechte anhaften, beispielsweise auf Eigentum, Rückzahlung oder einen Anteil an künftigen Gewinnen. Utility Tokens schließlich können gegen Zugriff auf ein bestimmtes Produkt oder eine Dienstleistung eingelöst werden und werden typischerweise über eine Blockchain-Plattform genutzt.

Der Bericht stellte klar, dass Kryptowährungen nicht den Kriterien herkömmlicher Währungen entsprechen. ICOs, Security Tokens und Utility Tokens bieten somit Möglichkeiten für Innovation und Effizienzen im Finanzsektor. Der Bericht empfiehlt auch, den Verkauf von Exchange-Token-Derivaten an Privatverbraucher zu verbieten. Ausgenommen von dieser Empfehlung sind Kryptowährungsderivate, die die Kriterien von Wertpapieren erfüllen, die allerdings Beschränkungen anderer Wertpapierbehörden wie der ESMA unterliegen könnten.

Financial Action Task Force

Im Juni 2015 gab die FATF Leitlinien über die Anwendung eines risikoorientierten Ansatzes zu Minderung der Geldwäsche- und Terrorismusfinanzierungsrisiken in Verbindung mit Kryptowährungen heraus. Die FATF-Leitlinien sollten zentrale und dezentrale Anbieter von Zahlungsprodukten und -dienstleistungen für Kryptowährungen anweisen, wie ein risikoorientierter Ansatz auf AML-/CTF-Prozesse angewandt werden kann, und wie die entsprechenden FATF-Empfehlungen umzusetzen sind.[6]

Im Oktober nahm die FATF offiziell eine Änderung an Recommendation 15 (New Technologies) vor. Recommendation 15 war ursprünglich auf die Minderung des Risikos ausgerichtet, das aus der Entwicklung und Anwendung neuer Technologien entstehen kann. Die Änderung im Oktober 2018 bezog sich spezifisch auf Kryptowährungen. Ländern wurde auferlegt, AML-/CTF-Vorschriften für Anbieter von Kryptovermögenswerten einzuführen. Das beinhaltet Börsen, bestimmte Arten von Wallet-Anbietern und Finanzdienstleistungsanbieter für ICO2s.[7]

Anbieter von Kryptovermögenswerten müssen darüber hinaus zugelassen und bei der zuständigen Aufsichtsstelle angemeldet sein, um ihrer Tätigkeit nachzugehen. Zu den wichtigen Konsequenzen für die Aufsichtsbehörde eines jeweiligen Rechtssystems zählt, ohne Einschränkung, die Kontrolle des Bestehens der Anbieter von Kryptovermögenswerten (beispielsweise Entzug von Lizenzen, Ablehnung von Lizenzanträgen, Verhindern, dass Verbrecher das wirtschaftliche Eigentum an Anbietern von Kryptovermögenswerten erlangen), die Überwachung der AML-/CTF-Compliance der Anbieter von Kryptovermögenswerten und die Anwendung von Strafmaßnahmen für die Nichteinhaltung.

Die FATF setzte Juni 2019 als den letztmöglichen Übernahmetermin der für Kryptowährungen vorgeschriebenen aufsichtsrechtlichen Auflagen fest. Die 40 Recommendations der FATF für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung gelten als globaler Standard. Diese Änderung ist wesentlich, um einen einheitlichen internationalen AML-/CTF-Ansatz für Kryptowährungen zu schaffen. Darüber hinaus können Länder, die die geänderte Recommendation 15 nicht einhalten oder nicht ausreichend umsetzen, eventuell als „hochriskant" eingestuft werden. Infolgedessen unterlägen sie höheren Überwachungsanforderungen seitens der mit den FATF-Auflagen konformen Ländern sowie Hindernissen beim Eröffnen von Vostrokonten bei großen, internationalen Banken. Anleitungen über die Verantwortlichkeiten der Anbieter von Kryptovermögenswerten können helfen, weltweit einheitliche AML-/CTF-Verfahren einzuführen. Ebenso wichtig ist jedoch, dass auf verdächtige Vorkommnisse hingewiesen wird, damit Anbieter von Kryptowährungen verdächtige Transaktionen konsequent an die Strafverfolgungsbehörden melden können. FATF-Standards sind bei der Gestaltung rechtlicher Vorschriften von großer Wichtigkeit. Deshalb ist es unerlässlich, die virtuelle Währungsindustrie ebenso wie Strafverfolgungsbehörden, herkömmliche Banken und nationale Aufsichtsbehörden einzubinden, um wirksame FATF-Recommendations zu erstellen.

Japan

Japan verfügt über einen der größten Kryptowährungsmärkte der Welt und hat Kryptowährungsbörsen proaktiv akzeptiert und beaufsichtigt. Das Land war aber auch Schauplatz einiger der größten Diebstähle von Kryptowährungen. Ein erheblicher Teil der 2018 von Börsen gestohlenen 950 Millionen $ Kryptowährung stammte aus Japan.[8] Die in Japan ansässigen Börsen Coincheck und Zaif[9] mussten aufgrund von Diebstahl Verluste von 530 Millionen $ beziehungsweise 60 Millionen $ in verschiedenen Tokens wegstecken. In Reaktion auf diese Attacken hat die Financial Services Agency der Kryptowährungsindustrie Selbstregulierungsstatus verliehen und die japanische Virtual Currency Exchange Association (JVCEA) als Selbstregulierungsgremium eingerichtet. Die Organisation erwägt jetzt das Auflegen einer Obergrenze von 10 bis 20 Prozent für Kundeneinlagen, die online in Hot Wallets (Wallets, deren Schlüssel online gespeichert sind) verwaltet werden können.[10] In Hot Wallets aufbewahrtes Geld ist für Hackerangriffe anfällig. Sicherheitsstandards für derartige Depotdienste können wesentlich zum Verbraucherschutz und zur Rufverbesserung in der Kryptowährungsbranche beitragen.

Die JVCEA gibt außerdem Business Improvement Orders heraus, die Strafzahlungen beinhalten können. Zaif hat bisher zwei Improvement Orders erhalten, eine auf „Einrichtung eines wirksamen Risikomanagementsystems" und eine zweite auf „Einrichtung eines Systems für angemessenes Eingehen auf Kundenanliegen". Eine weitere Kryptowährungsbörse, Quoine, hat nach eigenen Angaben eine Order in Bezug auf Compliance, KYC und AML erhalten. Die Einführung einer Überwachungsstelle, die das Sicherheitsniveau und die AML-Kontrollen japanischer Kryptobörsen übersieht und die entsprechenden Vorschriften durchsetzt, ist eine Präventionsmaßnahme gegen Mega-Diebstähle wie den 2018 in Japan.

Japan erlegt Kryptowährungsbörsen auch das Melden verdächtiger Aktivitäten auf. Laut japanischen Strafverfolgungsbehörden erhöhte sich die Anzahl der von

Kryptowährungsbörsen gemeldeten verdächtigen Transaktionen um ein Zehnfaches, nachdem im April 2017 ein Gesetz in Kraft trat, das Kryptowährungsbörsen zu entsprechenden Meldungen verpflichtet. Diese Vorschriften ebnen den Weg für die Zusammenarbeit zwischen auf Kryptowährungen basierenden Unternehmen und Strafverfolgungsbehörden zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung. Die Kryptowährungsbörse ShapeShift hatte 2018 laut eigenen Angaben bei 60 Anfragen von Strafverfolgungsbehörden weltweit geholfen, von denen 43 aus Ländern mit starken AML-Vorschriften kamen, darunter Deutschland, das Vereinigte Königreich, Frankreich, die USA, Kanada, die Schweiz, Australien und die Niederlande.

Malta

Kryptowährungen und Blockchain-Technologie bieten enorme Wachstumsmöglichkeiten im Finanzsektor ebenso wie in anderen Branchen. So überrascht es nicht, dass Länder weltweit darum wetteifern, Anbieter in diesem neuen Wachstumssektor anzuziehen. Unter den Kryptowährungen gegenüber aufgeschlossenen Nationen sticht Malta besonders hervor. Malta hat als erstes Land einen spezifisch für Kryptowährungen und Blockchain-Technologie konzipierten aufsichtsrechtlichen Rahmen eingeführt. Aufsichtsbehörden bemühen sich typischerweise, mit Kryptowährungen verbundene neue Risiken zu mindern, indem sie Kryptowährungen mit in die bestehenden aufsichtsrechtlichen Rahmenwerke für AML/CTF und Finanzwertpapiere aufnehmen. Der aufsichtsrechtliche Rahmen in Malta beinhaltet als einziger Richtlinien, die die Entwicklung von Blockchain-Technologie fördern. Dieser aufsichtsrechtliche Rahmen wird durch drei Gesetze geregelt: den Virtual Financial Assets Act (VFAA), den Malta Digital Innovation Authority Act (MDIA) und den Innovative Technology Arrangements and Services Act.[11]

Der VFAA regelt Compliance- und Zulassungsanforderungen für Kryptowährungs-Finanzdienstleister ebenso wie die verschiedenen Aspekte von ICOs, beispielsweise Verfahren für die Ausgabe und Anmeldung von Weißbüchern. Weiterhin untersagt der VFAA den Marktmissbrauch an Börsen und legt aufsichtsrechtliche und Ermittlungsbefugnisse fest. Mit dem MDIA wird die Malta Digital Innovation Authority ermächtigt, Richtlinien zu entwickeln und durchzusetzen, um die Entwicklung und Anwendung von Blockchains auf ethische und den aufsichtsrechtlichen Anforderungen entsprechende Art zu fördern. Der Innovative Technology Arrangements and Services Act legt den Rahmen für die freiwillige Zertifizierung innovativer Technologien fest (beispielsweise Software für Distributed-Ledger-Technologie, Smart Contracts etc.).

Die Risiken internationaler Geldwäsche infolge unzureichender Regeln

Im Juli 2017 erhob das US-Justizministerium Anklage gegen den russischen Staatsbürger Alexander Vinnik. Vorgeworfen wird ihm die angebliche Nutzung der BTC-e-Börse, um Verbrechenserlöse zu waschen, einschließlich Bitcoins aus dem berüchtigten Mt.-Gox-Hack, bei dem 850.000 Bitcoins von Benutzern der Börse gestohlen worden waren. In einer öffentlichen Mitteilung stellte das Justizministerium fest: „Laut Anklage haben Vinnik und andere seit der Gründung für BTC-e einen Kundenstamm aufgebaut, der zu großen Teilen aus Kriminellen bestand. Unter anderem wurden von Benutzern keine Identitätsnachweise verlangt, Transaktionen und Herkunft von Geldern wurden verborgen und anonymisiert, und es wurden keinerlei Anti-Geldwäsche-Verfahren befolgt.“[12] Kriminelle sollen diese Infrastruktur zur Handhabung und zum Erhalt von Geldmitteln aus Cyberverbrechen genutzt haben, darunter das Hacken von Kryptowährungen (Diebstahl), Ransomware-Attacken, Identitätsdiebstahl und eine Reihe von Betrugsfällen. Vinnik verwaltete demnach mehrere BTC-e-Konten ebenso wie Konten bei anderen Börsen, um die Spur gehackter Bitcoins zu verbergen, beispielsweise beim Mt.-Gox-Hack. Es ist möglich, dass diese anderen Börsen schwache oder überhaupt keine AML-Kontrollen anwandten. Berichten zufolge hatte BTC-e Bitcoins im Wert von 4 Milliarden $ erhalten, was die Dimension des Geschehens demonstriert.

Die Ermittlungen gegen Vinnik und seine Verhaftung waren das Resultat einer Zusammenarbeit mehrerer Staaten, so FBI Special Agent Amy Hess: „Die Verhaftung von Alexander Vinnik ist das Resultat einer multinationalen Aktion und demonstriert die Vorteile der weltweiten Kooperation zwischen US-amerikanischen und internationalen Strafverfolgungsbehörden.“[13] Die Leichtigkeit, mit der illegal erlangtes Vermögen mithilfe von Kryptowährungen überwiesen werden kann, ist ein weltweites Problem. Die Staaten müssen bei den Bemühungen zur Bekämpfung der Geldwäsche kooperieren. Bleiben solche Bemühungen jeweils in jedem Land isoliert, können Verbrecher mobil bleiben. Deshalb ist ein einheitlicher AML-Ansatz notwendig.

Ausblick

In den nächsten beiden Jahren wird sich die aufsichtsrechtliche Landschaft erwartungsgemäß erheblich verändern. Die von der FATF eingeführten Vorschriften sollen im Juni 2019 endgültig umgesetzt und rechtskräftig werden. Die 5AMLD soll bis Januar 2020 EU-weit umgesetzt werden. Diese Vorschriften könnten als ein Wachstumshindernis für die Kryptowährungsbranche gesehen werden. Kryptowährungen und die ihnen zugrundeliegende Blockchain-Technologie werden jedoch mit hoher Wahrscheinlichkeit weiter wachsen, wenn die Branche und Branchenakteure bei Regierungen, Aufsichtsbehörden, Finanzinstituten und in der Öffentlichkeit Vertrauen aufbauen können. Vertrauen ist möglich, wenn weltweite Mindeststandards in Verbindung mit lokalen Gesetzen, Vorschriften und Durchsetzungsbestimmungen die Grundlage für Rechenschaft und Verantwortung schaffen. Kryptowährungsunternehmen haben oft Probleme, die für nachhaltiges Geschäftswachstum notwendigen Bankverbindungen zu knüpfen und zu pflegen. Betreiber mit schwachen AML-/CTF-Kontrollen verschärfen dieses Problem für Anbieter, die ihrerseits angemessene Complianceprogramme verfolgen. Einheitliche Vorschriften mit Schwerpunkt auf öffentlicher Sicherheit, ohne dabei das Wachstum des Geschäfts und der Technologie zu behindern, können sowohl der Kryptowährungsbranche als auch der allgemeinen Öffentlichkeit zugute kommen. Effiziente und praktische Vorschriften, die auf Kenntnissen verantwortungsbewusster Kryptowährungsanbieter und Strafverfolgungsbehörden beruhen, werden den damit verbundenen Risiken von Geldwäsche und Terrorismusfinanzierung am besten gerecht.

Aufsichtsbehörden haben Maßnahmen ergriffen, um die mit Kryptowährungen verbunden Risiken zu mindern. Zu diesem Zweck werden Kontrollmaßnahmen für die Branche und Branchenakteure auferlegt. Ein einheitlicher Ansatz in Bezug auf weltweite Mindeststandards ist unerlässlich. Wichtig ist aber auch, dass Aufsichtsbehörden ihre Regelwerke auf das Mindern der für Kryptowährungen einzigartigen Risiken ausrichten. Das Durchsetzen bestehender Standards aus der herkömmlichen Finanzbranche ist bei Kryptowährungen nicht immer angebracht. Es kann das Wachstum behindern und eventuell sogar zu unnötigen Meldungen und den damit verbundenen Datenschutzproblemen führen. Vorschriften für Kryptowährungen sollten auf einem stimmigen Ausgangspunkt beruhen. Langfristig ist jedoch ein flexibler und weitsichtiger Ansatz, der Technologieinnovationen entsprechend angepasst werden kann, wahrscheinlich effizienter als ein „one-size-fits-all"-Ansatz. A

Julian Arriagada, CAMS, manager compliance, Tether, Julian@tether.to

Yasmine Ibrahim, analyst compliance, Tether, Yasmine@tetehr.to

Contributor: Leonardo Real, chief compliance officer, Tether, Leo@tether.to

[1] "Cryptocurrency Anti-Money Laundering Report 2018 Q3," CipherTrace, 2018, https://ciphertrace.com/crypto-aml-report-2018q3.pdf

[2] "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," Financial Crimes Enforcement Network, 18 March 2013, https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf

[3] "Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses," U.S. Department of the Treasury, 28 November 2018, https://home.treasury.gov/news/press-releases/sm556

[4] Matthew Allen, "Crypto Fund wins first Swiss crypto asset management licence," *Swissinfo*, 9 October 2018, https://www.swissinfo.ch/eng/finma-breakthrough_crypto-fund-wins-first-swiss-crypto-asset-management-license/44461088

[5] Ana Alexandre, "New Study Says 80 Percent of ICOs Conducted in 2017 Were Scams," *Cointelegraph*, 13 July 2018, https://cointelegraph.com/news/new-study-says-80-percent-of-icos-conducted-in-2017-were-scams

[6] "Guidance for a Risk-Based Approach to Virtual Currencies," Financial Action Task Force, June 2015, http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html

[7] "Outcomes FATF Plenary, 17-19 October 2018," Financial Action Task Force, 19 October 2018, http://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-plenary-october-2018.html

[8] "Cryptocurrency Anti-Money Laundering Report 2018 Q4," CipherTrace, 2018, https://ciphertrace.com/wp-content/uploads/2019/01/crypto_aml_report_2018q4.pdf

[9] "Cryptocurrency Anti-Money Laundering Report 2018 Q3," CipherTrace, 2018, https://ciphertrace.com/crypto-aml-report-2018q3.pdf

[10] Erik Gibbs,"JVCEA to tighten crypto storage regulations," Squire Mining, https://squiremining.com/category/japan-virtual-currency-exchange-association/

[11] "FinTech," Malta Financial Services Authority, https://www.mfsa.com.mt/fintech/

[12] "Russian National and Bitcoin Exchange Charged In 21-Count Indictment For Operating Alleged International Money Laundering Scheme and Allegedly Laundering Funds From Hack Of Mt. Gox," The United States Attorney's Office Norther District of California, 26 July 2017, https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged

[13] "Russian national and bitcoin exchange indicted in multi-billion dollar money laundering scheme," U.S. Immigration and Customs Enforcement, 26 July 2017, https://www.ice.gov/news/releases/russian-national-and-bitcoin-exchange-indicted-multi-billion-dollar-money-laundering

FINTECH: FREUND oder FEIND bei der Aufdeckung und Prävention von Finanzkriminalität?

Anmerkung des Verfassers: In diesem Artikel bezieht sich der Begriff „Fintechs" spezifisch auf Anbieter digitaler Bankkonten (beispielsweise Monzo) und anderer E-Wallet-Dienste (beispielsweise Apple Pay).

Fintechs sind Anbieter digitaler Bankkonten und E-Wallets. Eine zunehmende Anzahl von Marktakteuren bietet Zahlungskonten, Geldtöpfe oder Überweisungsdienste auf digitaler Grundlage an. Neu ist die Tatsache, dass auch die Akzeptanz bei Endbenutzern rapide steigt.[1] Kaum eine Woche vergeht ohne Medienberichte über Challenger-Banken (auch „Neobanken" genannt) wie Monzo, Revolut oder N26, die zunehmend mehr Kunden anwerben.[2]

Andererseits scheinen herkömmliche Bankinstitute Kunden nicht in beunruhigendem Ausmaß zu verlieren. Was genau passiert also? Warum gibt es keinen reinen Übergang von Traditionsbanken zu Fintechs?

Kunden nutzen die neuen Zahlungssysteme und Plattformen, ohne ihre traditionelle Bank zu verlassen.[3]

Die Erklärung dafür liegt auf der Hand. Je nach Situation und Finanzgebaren hat jeder eigene Gründe dafür, Konten sowohl bei einer traditionellen Bank als auch bei einem Fintech zu führen. Wenn Kunden zu Fintech-Banken wechseln, kündigen sie tatsächlich häufig ihre „herkömmlichen" Bankkonten nicht. Stattdessen werden beide Arten von Konten für verschiedene Zwecke geführt. Eventuell brauchen Benutzer beispielsweise eine Möglichkeit, ihre Fintech-Konten zu finanzieren. In diesem Fall werden herkömmliche Bankkonten nur genutzt, um digitalen Konten Mittel zuzuführen. Oder vielleicht bietet die traditionelle Bank Dienstleistungen an, die der Fintech-Anbieter noch nicht zur Verfügung stellt, beispielsweise Investments, Darlehen etc. Es ist auch möglich, dass neue Benutzer ihrem Fintech-Kontoanbieter noch nicht voll vertrauen. In der Europäischen Union (EU) muss ein Fintech-Kontoanbieter zuerst eine Banklizenz erhalten, bevor die von Kunden hinterlegten Mittel durch die EU-Einlagensicherung[4] geschützt sind, die Spareinlagen von bis zu 100.000 Euro ($113.000) garantiert.

Einige Benutzer nennen aber auch die Benutzerfreundlichkeit, wettbewerbsfähige Preise und bessere Servicequalität als Gründe für den Wechsel zu Fintech-Konten.[5]

Es stellt sich die Frage, ob die unzähligen Möglichkeiten, dank derer jetzt nahezu jeder ein Fintech-Konto eröffnen und binnen Minuten Zahlungen (typischerweise über eine Zahlungskarte) durchführen kann, die Finanzkriminalität begünstigen.

Mehr Aufmerksamkeit für die Rolle der Fintechs in der Finanzkriminalität

Wie viele Leser verfügen bereits über ein Fintech-Konto? Fachkräfte für die Geldwäscheprävention (AML) dürften sich für diese (manchmal nur vorgeblich) disruptiven Methoden interessieren, mit denen Kundenanmeldungen, das Einholen und Überprüfen von Identitätsnachweisen und Know-Your-Customer-Prüfungen (KYC) allgemein durchgeführt werden. Eventuell haben sie sogar selbst mehr als ein Konto bei Fintechs oder Challenger-Banken. Welche Informationen werden also angefordert, wenn jemand sich für ein neues Konto anmeldet?

Im Wesentlichen sind dies bei allen Anbietern dieselben Informationen: personenbezogene Daten, belegt durch ein amtliches Identitätsdokument, und manchmal die staatliche Steuernummer, für die kein Beleg erforderlich ist.

Eine Person kann praktisch so viele Konten eröffnen, wie es Fintech-Anbieter gibt. Was ist der Unterschied zwischen herkömmlichen Finanzinstituten und Fintechs?

Die Eröffnung eines Bankkontos in einem Nicht-Wohnsitzland, in dem auch kein Einkommen erzielt wird, dauert erheblich länger als nur einige Minuten.

Tatsächlich fordern die meisten EU-Banken beim Eröffnen eines Kontos durch eine nicht im Land ansässige Person, auch bei EU-Bürgern, folgende Informationen an:

- Beschäftigungsnachweis (Arbeitsvertrag oder Nachweis der Unternehmensgründung bei Selbständigen)
- Anmeldebescheinigung des Wohnsitzlandes
- andere üblicherweise angeforderte Informationen und Unterlagen (in der Regel ein Identitäts- und ein Adressnachweis)

Ein Anreiz für Kriminelle, das herkömmliche Bankensystem aufzugeben

Neuere Schlagzeilen scheinen zu bestätigen, dass staatliche Behörden die herkömmlichen Banken unter enormen Druck setzen, ihre AML-Kontrollen zu verstärken.

Neu hinzukommende Zahlungsanbieter benötigen zwar Lizenzen (meistens Lizenzen für Zahlungs- oder E-Geld-Institute) und entwickeln sich somit nicht in einem gesetzlich ungeregelten Rahmen. Die EU-Verordnung über den grenzüberschreitenden Pass-Mechanismus ermöglicht neuen Zahlungsanbietern jedoch die Option, in einer beliebigen Region des Europäischen Wirtschaftsraums tätig zu sein, ohne im gleichen Staat der Aufsicht zu unterliegen.

Damit wird es für Aufsichtsbehörden im Heimat- ebenso wie im Gastgeberland sehr viel schwieriger, Aktivitäten in der gesamten EU zu überwachen, besonders ohne eine EU-weite Aufsichtsstelle. Dies wissen auch mögliche Finanzverbrecher.

Falls ein Krimineller beispielsweise illegal erlangtes Geld in Höhe von 100.000 Euro ($113.000) verbergen möchte, könnte er einfach den oben beschriebenen, einfachen Kontoeröffnungsprozess durchlaufen. Das Eröffnen von Konten bei zehn verschiedenen Fintech-Kontoanbietern, die jeweils in einem anderen EU-Staat zugelassen sind, dauert mit einem Smartphone und Identitätsbeleg nur rund 5 bis 10 Minuten pro Konto. Selbst wenn das Fintech ordnungsgemäße Maßnahmen für die Geldwäsche-Prävention (AML) und Anti-Terrorismusfinanzierung (CTF) durchführt, wird ein Krimineller, falls er nicht mehr als 10.000 Euro ($11.300) auf jedes Konto einzahlt, wahrscheinlich nicht um weitere Informationen oder Unterlagen gebeten.

Stellen wir uns jetzt vor, dieser Verbrecher möchte nicht 100.000 Euro, sondern stattdessen 1.000.000 Euro ($1.131.000) verstecken. Er würde noch immer verschiedene Konten bei insgesamt zehn Fintechs eröffnen, die in einem jeweils anderen EU-Staat zugelassen sind. Anstatt 10.000 Euro würde er aber auf jedes Konto 100.000 Euro einzahlen, jeweils in mehrere kleinere Einlagebeträge aufgeteilt.

Dies sollte hoffentlich im Überwachungssystem jedes Fintechs ein Alarmsignal auslösen. Eventuell wird der Kriminelle sogar ersucht, die Herkunft dieser Mittel zu erklären und zu belegen. Zusätzlich reichen die AML-Teams dieser Fintechs eventuell sogar eine Meldung verdächtiger Transaktionen bei der zuständigen Financial Intelligence Unit (FIU) ein. Aber was geschieht dann?

Zehn verschiedene FIUs in zehn verschiedenen EU-Ländern werden unabhängig voneinander darüber informiert, dass eine Person strukturierte Einzahlungen auf ein Konto bei einem in dem jeweiligen Staat (beispielsweise mit einer Lizenz als Zahlungsinstitut, E-Geld-Institut oder Spezialbank) zugelassenen Fintech vornimmt.

Angesichts der aktuellen Arbeitslast von FIUs in ganz Europa ist es unwahrscheinlich, dass diese Information—die nicht im Zusammenhang mit eventuellen Geschehnissen in anderen europäischen Ländern wahrgenommen werden kann—zu einer weitergehenden Ermittlung führt.

Zudem können die einzelstaatlichen FIUs sich noch immer nicht an eine EU-weite FIU wenden, in der die aus allen Mitgliedstaaten erhaltenen Informationen zentral erfasst werden.

Die Risiken von Fintechs und Challenger-Banken im Hinblick auf Finanzkriminalität zeigen sich also eindeutig an der Leichtigkeit, mit der binnen Minuten Konten in ganz Europa eröffnet werden können.

Kryptovermögen: rechtliche Unsicherheit, die Kriminellen zugute kommt

Angenommen, die erwähnten Fintech-Kontoanbieter unterliegen größtenteils der Finanzaufsicht. Sie müssen dieselben AML/CTF-Anforderungen erfüllen wie herkömmliche Banken. Für Anbieter von Kryptovermögen (Anbieter von Börsen, E-Wallets etc.) trifft dies im EU-weiten Rahmen noch nicht zu. Die folgenden Maßnahmen, die derzeit für Fintechs erwogen werden, gelten somit eventuell für Anbieter von Kryptovermögen noch nicht:

- KYC-Sorgfaltspflicht in Bezug auf Kunden
- AML/CTF-Transaktionsüberwachung
- Meldungen verdächtiger Transaktionen

Tatsächlich (und erfreulicherweise) wenden die größeren Anbieter von Kryptovermögen die entsprechenden Regeln bereits an. Das geschieht nicht nur aus Verantwortungsbewusstsein, sondern auch, weil sie ohne diese Maßnahmen kaum mit den Finanzinstituten zusammenarbeiten könnten, mit denen sie zur Erleichterung ihrer Tätigkeiten Partnerschaften schließen.

Mit welchen Lösungen kann dieser neuen Gefahr begegnet werden?

Aus Sicht der Behörden

Ungeachtet mehrerer aufeinanderfolgender EU-Anti-Geldwäscherichtlinien könnte der EU-Pass-Mechanismus—angesichts der noch immer erheblichen Unterschiede zwischen AML/CTF-Vorschriften und ihrer Durchsetzung in den verschiedenen Mitgliedstaaten—die übergreifenden AML/CTF-Maßnahmen sogar schwächen.

Um das Risiko zu verringern, dass illegales Geld über verschiedene, nicht ausreichend wachsame und/oder überwachte Online-Zahlungsanbieter verteilt wird, könnten EU-Behörden beispielsweise die Befugnisse nationaler Aufsichtsstellen erweitern. Zudem könnte die Einrichtung einer gemeinsamen, EU-weiten Aufsichtsinstanz den Übergang von einem relativ einheitlichen Aufsichtsrechtsrahmen hin zu einer einheitlicheren Rechtsdurchsetzungspolitik ermöglichen.

Aus Sicht der Fintechs

Wie erwähnt werden Fintech-Konten typischerweise als Zusatzkonten und nicht als Hauptbankverbindung genutzt. Dementsprechend könnten Überwachungsmuster und Alarmsignale konzipiert werden.

So finanzieren zum Beispiel die meisten Kunden ihre Fintech-Konten über ihre regulären Bankkonten und verwenden diese Guthaben dann direkt in ihren Apps für Überweisungen an Freunde und Familienmitglieder. Falls Kunden nur Mittel von Konten erhalten, die nicht in ihrem Besitz befindlich sind, und diese dann direkt auf andere Konten überweisen ohne anderweitig Fintech-Produkte zu nutzen, wäre es also sinnvoll, nachzufassen.

Fazit

Fintech-Kontoanbieter (Fintechs) und neu aufkommende Zahlungssysteme sind faszinierend, weil sie Finanzprodukte entmystifizieren, den Wettbewerb im Ökosystem der Finanzdienstleistungen (der lange Zeit wenigen Anbietern vorbehalten war) für neue Akteure öffnen und letztendlich den Kunden wieder in den Mittelpunkt des Leistungsangebots rücken.

Angesichts von Technologie, Innovation und Diskontinuität dürfen wir aber nicht aus den Augen verlieren, dass diese gerade erst aufkommenden Akteure noch Neulinge im Bereich „Compliance-Kultur“ sind und noch wenig Erfahrung haben, sich in einem beständig entwickelnden aufsichtsrechtlichen Umfeld zu bewegen.

Auch wenn viel über neue Schwächen und die Versäumnisse der etablierten EU-Bankinstitute bekannt wird, sollten wir darüber nicht vergessen, dass die neuen Marktteilnehmer, wie positiv und wohlmeinend sie auch sein mögen, ebenfalls sorgfältiger Überwachung bedürfen.

Alexandre Pinot, CAMS, head of Vilnius office and MLRO, SONECT Europe, Vilnius, Lithuania, alexandre@sonect.ch

[1] “EY Fintech Adoption Index 2017: The rapid emergence of Fintech,” EY, 2017, https://www.ey.com/Publication/vwLUAssets/ey-Fintech-adoption-index-2017/$FILE/ey-Fintech-adoption-index-2017.pdf

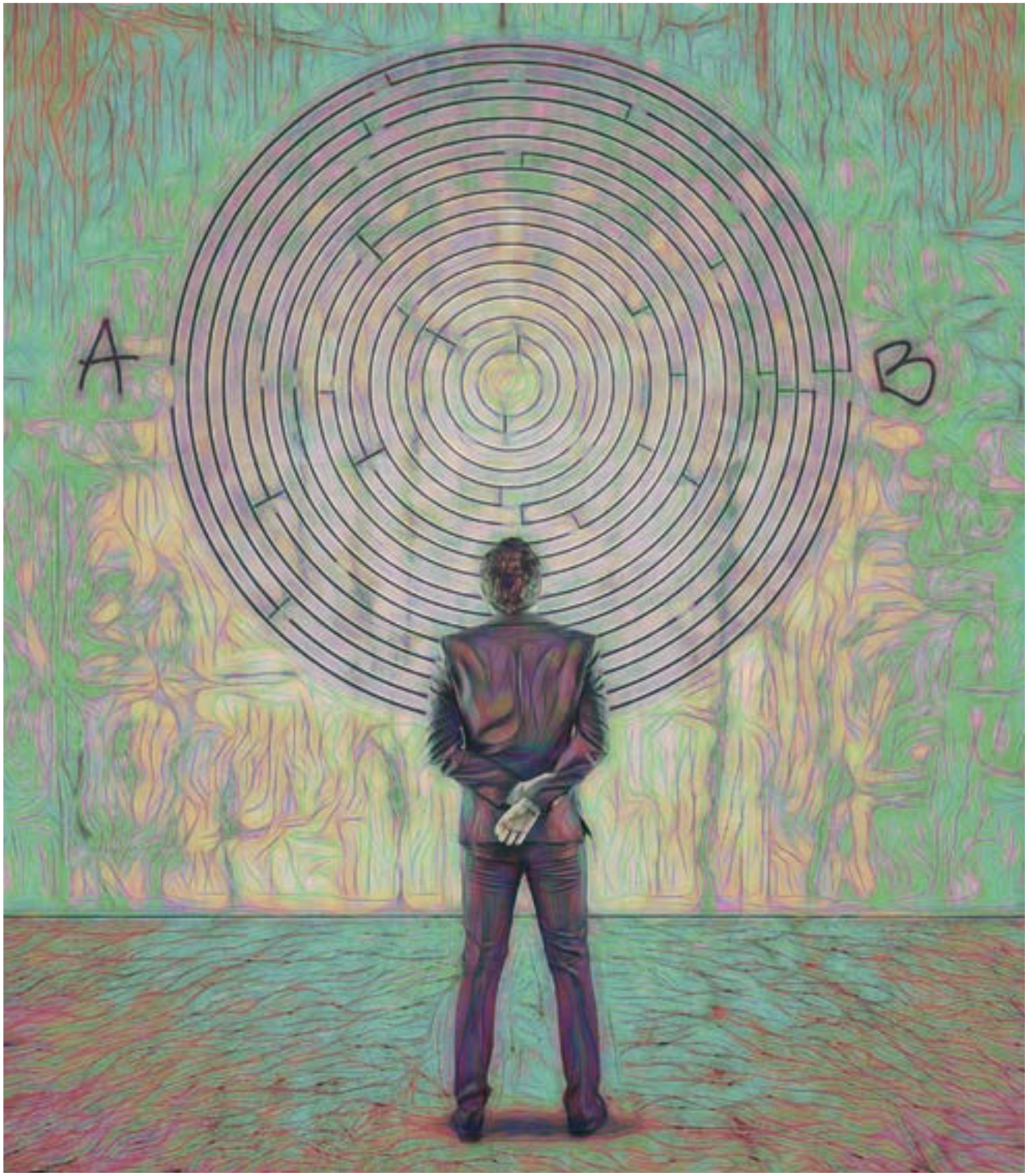
[2] “Neo and Challenger Bank Customer Base to Grow by 50.6%, Globally, by 2020,” Allied Market Research, https://www.alliedmarketresearch.com/press-release/neo-and-challenger-bank-market.html

[3] Oliver Smith, “A Million U.K. Consumers Just Switched Their Bank Accounts—But Not To Fintech Challengers” *Forbes*, 26 July 2018, https://www.forbes.com/sites/oliversmith/2018/07/26/a-million-u-k-consumers-switched-their-bank-accounts-but-not-to-fintech-challengers/#7932444c1205

[4] “Deposit guarantee schemes,” European Commission, https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/managing-risks-banks-and-financial-institutions/deposit-guarantee-schemes_en

[5] Jeff Desjardins, “How Fintech is Digitally Disrupting the Financial World,” Visual Capitalist, 3 August 2016, https://www.visualcapitalist.com/how-Fintech-digitally-disrupting-financial-world/

RISKANTE GESCHÄFTE:
5AMLD und die verstärkte Sorgfaltspflicht



Die fünfte Anti-Geldwäsche-Richtlinie der Europäischen Union (5AMLD)[1] wurde am 9. Juli 2018 verabschiedet und muss bis zum Januar 2020 von allen EU-Mitgliedstaaten umgesetzt werden. Von der neuen Richtlinie betroffene Unternehmen, sogenannte Verpflichtete, müssen sich mit neuen Herausforderungen auseinandersetzen, die aus den relevanten Änderungen der vierten Anti-Geldwäsche-Richtlinie der Europäischen Union (4AMLD) aus dem Jahr 2015 (umgesetzt 2017) hervorgehen.[2]

Geschäftsbeziehungen in Drittländern mit hohem Risiko, Länder die laut Bewertung der Europäischen Kommission strategische Mängel bei der Prävention von Geldwäsche und Terrorismusfinanzierung [AML/CTF] aufweisen, sind von besonderem Belang.[3] Die neue Richtlinie fordert eine verstärkte Sorgfaltspflicht (Enhanced Due Diligence, EDD) und empfiehlt eine eventuelle Beschränkung der Geschäfte mit Hoch-Risiko-Ländern (siehe Kasten 2). Die Auswahl der Länder für diese Schwarzliste hat sich allerdings als politisch kontrovers erwiesen (siehe Kasten 1).

KASTEN 1

Maßnahmen für die verstärkte Sorgfaltspflicht in Bezug auf Drittländer mit hohem Risiko

Artikel 18a (Richtlinie (EU) 2018/843) erfordert einheitliche Maßnahmen im Rahmen der verstärkten Sorgfaltspflicht, einschließlich der Einholung zusätzlicher Informationen über den Kunden und die wirtschaftlichen Eigentümer; die angestrebte Art der Geschäftsbeziehung; die Herkunft der Gelder und des Vermögens des Kunden und die Gründe für die geplanten oder durchgeführten Transaktionen.

Als eine mögliche Vorsichtsmaßnahme gilt, dass die „erste Zahlung über ein Konto im Namen des Kunden bei einem Kreditinstitut [erfolgt], das Sorgfaltspflichten unterliegt, die nicht weniger strikt sind als die in dieser Richtlinie festgelegten."

Zusätzlich zur verstärkten Überwachung der Geschäftsbeziehung und der risikomindernden Maßnahmen bei Transaktionen mit Ländern mit hohem Risiko, empfiehlt die Richtlinie gegebenenfalls Einschränkungen der Geschäftsbeziehungen, beispielsweise die ‚Verwehrung der Gründung von Tochtergesellschaften, Zweigniederlassungen oder Repräsentanzbüros von Unternehmen aus einem Drittland mit hohem Risiko' und das ‚Verbot der Gründung von Tochtergesellschaften, Zweigniederlassungen oder Repräsentanzbüros' in dem betreffenden Land.

Eine weitere Klausel legt fest, dass Korrespondenzbankbeziehungen zu Respondenzinstituten in einem Drittland mit hohem Risiko zu überprüfen und zu ändern oder erforderlichenfalls zu beenden sind.

KASTEN 2

Kontroverse Liste der Drittländer mit hohem Risiko

Gemäß Artikel 9 (2) der Richtlinie (EU) 2018/843 legte die Europäische Kommission am 13. Februar 2019 eine Liste von 23 Drittländern mit hohem Risiko vor, die laut Bewertung strategische AML-/CTF-Mängel aufweisen.[4] Die Liste ging über die FATF-Liste von Ländern mit hohem Risiko, die überwacht werden, hinaus. Sie beinhaltet 11 weitere Länder oder Territorien, darunter Saudi-Arabien, Panama und drei U.S.-Territorien: Puerto Rico, Amerikanisch-Samoa und die Amerikanischen Jungferninseln. Das U.S.-Finanzministerium kritisierte die Liste.[5] Gleichzeitig wurde die Liste auch für die Auslassung einer Reihe von Ländern kritisiert, die den Kritikern zufolge aufgenommen hätten werden sollen.[6] Vor allem unterstützte der Europäische Rat die Liste nicht, sondern gab am 5. März 2019 seinen Einspruch bekannt.[7] Offiziell wurde der Einspruch mit methodischen Einwänden begründet. Allerdings erklärte die Kommission in ihrer Empfehlung—C(2019)1326—ihre Gründe für die Auswahl jedes Landes. Auch waren die betroffenen Länder angeblich vor Aufnahme in die Liste konsultiert worden.[8]

Die Streitigkeiten über die Liste der Länder mit hohem Risiko widersprachen dem eigentlichen Vorhaben einen harmonisierten Ansatz beim Umgang mit Ländern mit hohem Risiko anzustreben, bei dem der Schwerpunkt auf verstärkten Sorgfaltspflichten und risikomindernden Maßnahmen (falls anwendbar) liegen sollte. Aktuell überdenkt die Kommission die Liste. Sie wird frühzeitig die Zustimmung sowohl des Europäischen Rats als auch des Europäischen Parlaments erlangen müssen, mit dem Risiko einer letztendlich verwässerten Liste, die die Glaubwürdigkeit des ganzen Prozesses in Frage stellen würde.

Am 12. März 2019 aktualisierten die EU-Finanzminister ihre Liste nicht-kooperativer Länder und Gebiete für Steuerzwecke, die jetzt Amerikanisch-Samoa, Bahrain, Aruba, Barbados, Belize, Bermuda, Dominica, Fidschi, Guam, die Marshallinseln, Oman, Samoa, Trinidad und Tobago, die Amerikanischen Jungferninseln, die Vereinigten Arabischen Emirate und Vanuatu einschließt.[9] Es bleibt fraglich, ob diese Liste als vollständig und maßgeblich gelten kann oder aus politischen Gründen gekürzt ist. Zudem sind auf der Liste taktvollerweise keine EU-Mitgliedstaaten aufgeführt, die unter steuerlichen Gesichtspunkten als problematisch angesehen werden.

Finanzinstitute und andere Verpflichtete sollten beachten, dass politische Verhandlungen über solche Länderlisten nicht unbedingt nach objektiv gültigen Kriterien geführt werden und die tatsächlichen Verhältnisse eventuell nicht genau reflektieren. Unternehmen sollten daher jede von der EU oder beispielsweise von der Financial Action Task Force (FATF) erstellte Liste durch eine eigene Länderrisikoanalyse ergänzen, in der ihre Operationsgebiete sowie zuverlässige Experten- und Medienberichte zu relevanten AML-Mängeln berücksichtigt werden. Dies gilt ebenso für mögliche Verbindungen zu Steueroasen, die auf einer separaten EU-Länderliste aufgeführt sind.

Dieser Artikel geht auf einige weitere Änderungen der 5AMLD ein, die wesentliche Konsequenzen für die risikoorientierte Kundensorgfaltspflicht (CDD) haben.

Zentrale Informationen zu Eigentümer-Strukturen

Die 5AMLD legt regulatorische Verbesserungen fest, um die grundlegende Kundensorgfaltspflicht zu erweitern und insbesondere das Feststellen der wirtschaftlichen Eigentümer relevanter juristischer Personen zu ermöglichen. Die Register wirtschaftlicher Eigentümer in den EU-Mitgliedstaaten sollen künftig zentralisiert, erweitert und für die Öffentlichkeit leichter zugänglich werden. Grundsätzlich sollen die Register bis zum März 2021 über die zentrale Europäische Plattform vernetzt werden. Danach ist diese Plattform vor dem Eingehen einer neuen Geschäftsbeziehung verbindlich zu prüfen. Trusts und ähnliche Strukturen werden ebenfalls auf der zentralen Plattform für die Register wirtschaftlicher Eigentümer erfasst. Entgegen der aktuellen Praxis in einigen Mitgliedstaaten werden die Eigentümerinformationen für die Öffentlichkeit zugänglich sein, vorbehaltlich einiger Einschränkungen bei Trusts. Im Wesentlichen ist damit größere Transparenz für die Presse und Organisationen der Zivilgesellschaft möglich.

Sollte die EU die zentrale Datenbankplattform mit zuverlässigen Eigentümerinformationen wirksam realisieren, könnten die Konsequenzen weit über die verbesserte Effizienz von Know-Your-Customer-Nachforschungen (KYC) hinausgehen. Jedes Land, das diese Eigentümerinformationen nicht verfügbar macht, wäre nämlich aufsichtsrechtlich als ein Land mit hohem Risiko einzustufen. Praktisch gesehen bedeutete dies, dass KYC-Ermittlungen, die beim Feststellen der wirtschaftlichen Eigentumsverhältnisse über öffentliche Register auf Hindernisse stoßen, risikobasierte Maßnahmen zur verstärkten Sorgfaltspflicht auslösen, oder sogar die nächste Stufe der Integrity-Due-Diligence (IDD) mit Nachforschungen im betreffenden Land.

Der Kampf gegen die Geldwäsche beinhaltet strategische Interaktionen. Die regulatorische Verschärfung hat wahrscheinlich zur Folge, dass potenzielle Täter erfindungsreicher vorgehen anstatt einfach aufzugeben. Falls ein tatsächlicher wirtschaftlicher Eigentümer (englisch, Ultimate Beneficial Owner, UBO) verborgen bleiben möchte, wird er entweder Länder mit Rechtssystemen nutzen, die keine Eigentümerinformationen offenlegen, oder sich hinter vielschichtigen und komplexen Gesellschafterstrukturen verstecken. In jedem Fall sollten intransparente Strukturen, die eine Identifikation des wirtschaftlichen Eigentümers verhindern, künftig eine höhere Risikobewertung bewirken.

Transparenz von Geldmitteln

Weiterhin erlegt die 5AMLD in einem neuen Artikel 10 (1) den Mitgliedstaaten auf, ihren Kredit- und Finanzinstitute das Führen anonymer Konten, Sparbücher oder Schließfächer zu verbieten. Somit unterliegen die entsprechenden Inhaber und Begünstigten der Kundensorgfaltspflicht (diese Regelung ist seit dem 10. Januar 2019 wirksam). Außerdem wird bis zum September 2020 ein zentraler automatischer Mechanismus eingerichtet, der die Identifizierung der Inhaber von Bank- und Zahlungskonten und Schließfächern ermöglicht. Diese Informationen werden für die staatlichen Financial Intelligence Units (FIU) sowie relevante Behörden verfügbar sein.

Durch das Verbot anonymer Konten wird es einfacher, die Herkunft der Gelder eines Kunden herauszufinden. Beim Eingehen einer Geschäftsbeziehung sollte die Herkunft der Gelder immer eindeutig feststehen. Im Hinblick auf Drittländer, in denen aufgrund von Anonymität oder anderen Hindernissen die Herkunft von Geldmitteln nicht festgestellt werden kann, sollte ein derartiger Risikofaktor zur Anwendung der verstärkten Sorgfaltspflicht führen, bis hin Klärung der Herkunft des Vermögens des Kunden insgesamt.

Um festzustellen, ob Gelder aus illegal erwirtschafteten Mitteln stammen und/oder als Teil eines Geldwäschevorhabens überwiesen werden, muss der Fluss der Gelder im Zusammenhang mit der Art der Geschäftsbeziehung und dem Zweck der Transaktion bewertet werden. Jeder Verdacht, dass an einer Transaktion Mittelsleute beteiligt sind—hinter denen sich die Eigentümer potenziell illegaler Geldern verbergen könnten—ist ein Warnsignal und sollte zur Anwendung der verstärkten Sorgfaltspflicht führen.

Politisch exponierte Personen

Ein weiterer Bereich, in dem die 5AMLD Verbesserungen bei der Wahrnehmung der Kundensorgfaltspflichten einführt, betrifft die politisch exponierten Personen (PEPs). Die Mitgliedstaaten werden nunmehr verpflichtet, eine Liste bestimmter Ämter oder Positionen (ohne Namen) zu erstellen, die als wichtige öffentliche Funktionen in dem betreffenden Landes angesehen werden, einschließlich in dort registrierten internationalen Organisationen. Es bleibt abzuwarten, inwieweit die Klassifizierung von PEPs, beispielsweise im Hinblick auf führende Parteiämter oder Bürgermeisterposten in größeren Städte, auf diesen Listen unterschiedlich ausfällt. In jedem Fall sollte das Erkennen einer PEP oder eines Angehörigen oder einer nahestehenden Person einer PEP im Zusammenhang mit einer Kundenbeziehung bereits Teil der vereinfachten Sorgfaltspflicht sein, so dass bei

Vorliegen diese Risikofaktors entsprechende Maßnahmen im Rahmen der verstärkte Sorgfaltspflicht eingeleitet werden können.

Zunächst kann dabei auf vorbereitete PEP-Listen zugegriffen werden, was aber eventuell nicht ausreicht, da indirekte aber wesentliche Beziehungen zu PEPs über ihnen nahestehende Personen möglicherweise nicht aufgedeckt werden. PEPs dürften sich zunehmend bewusst sein, dass sie unter Beobachtung stehen. Auch hier gilt, dass diejenigen, die etwas zu verbergen haben, wahrscheinlich Vermittler benutzen werden, um keine Alarmsignale auszulösen.

Die verstärkte Sorgfaltspflicht in Bezug auf eine identifizierte PEP beinhaltet das Einholen zusätzlicher Informationen darüber, ob eine Einstufung als hohes Risiko gerechtfertigt ist—beispielsweise durch den Nachweis relevanter Geschäftsinteressen, fragwürdiger Machtausübung, sowie Verbindungen zu irregulären oder sogar korrupten Praktiken. All dies erhöht die Wahrscheinlichkeit einer Beteiligung an Geldwäscheaktivitäten. Die Definition einer PEP basiert auf ihrer Funktion. Sie muss im Kontext des jeweiligen politischen Systems und der betreffenden Geschäftsbeziehung betrachtet werden. Die Schwelle für das Definieren einer Person mit einer politischen Funktion als eine PEP sollte eher niedrig angesetzt werden, damit geeigneten Maßnahmen im Rahmen der Sorgfaltspflicht getroffen werden können, um Korruption und Geldwäsche gegebenenfalls festzustellen.

Fazit

Mit der 5AMLD werden die Anforderungen für die Umsetzung der verstärkten Sorgfaltspflicht bei Kunden mit hohem Risiko erneut heraufgesetzt. Zwar kämpft die EU noch mit politischen Schwierigkeiten, Länder mit hohem Risiko aufgrund strategischer Defiziten bei der Bekämpfung von Geldwäsche, Terrorismusfinanzierung und Steuerhinterziehung zu definieren. Allerdings bietet die kontroverse Debatte über die entsprechende Länderlisten Finanzinstituten und anderen Verpflichteten reichlich Informationen über bedenkliche Länder, die bei der Ausübung der Sorgfaltspflicht gegenüber mit diesen Ländern verbundene Kunden kaum ignoriert werden können. Im Hinblick auf die Überprüfung von Kundeninformationen geht aus der 5AMLD klar hervor, dass das Eingehen einer Geschäftsbeziehung ohne Kenntnis des wirtschaftlichen Eigentümers oder der Herkunft der Gelder ernsthafte Risiken einer Verbindung zu Verbrechern und illegalen Erlösen mit sich bringt. Im Rahmen der verstärkten Sorgfaltspflicht sollten vielschichtige Eigentümerstrukturen und Mittelsleute, die in Transaktionen eingeschaltet sind berücksichtigt werden. Ebenso erfordert das Identifizieren der versteckten Beteiligung einer PEP an Eigentumsverhältnissen und seiner Mitwirkung an Transaktionenen eingehende Kenntnis des politischen und geschäftlichen Umfelds eines Kunden. A

Dr. Carsten Giersch, senior partner, Berlin Risk Ltd., Berlin, Germany, carsten.giersch@berlinrisk.com

[1] "Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU," EUR-Lex, 30 May 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843

[2] "Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC," EUR-Lex, 20 May 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849

[3] "EU Policy on High-Risk Third Countries," European Commission, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/anti-money-laundering-and-counter-terrorist-financing/eu-policy-high-risk-third-countries_en; "EU Methodology for Identifying High-Risk Third Countries," Global Risk Affairs, 11 July 2018, https://www.globalriskaffairs.com/2018/07/eu-methodology-for-identifying-high-risk-third-countries/

[4] "Commission Delegated Regulation (EU) of 13.2.2019 supplementing Directive (EU) 2015/840 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies," European Commission, 13 February 2019, https://ec.europa.eu/info/sites/info/files/commission-delegated-regulation_hrtc.pdf

[5] "Treasury Statement on European Commission List of Jurisdictions with Strategic AML/CFT Deficiencies," U.S. Department of the Treasury, 13 February 2019, https://home.treasury.gov/news/press-releases/sm610

[6] Simon Bowers, "European Commission shames Saudi Arabia, Panama with 'dirty money' blacklist," *International Consortium of Investigative Journalists,* February 14, 2019, https://www.icij.org/blog/2019/02/european-commission-shames-saudi-arabia-panama-with-money-laundering-and-terror-financing-blacklist-but-attracts-criticism/

[7] Council of the European Union, 6964/1/19 REV 1; Bjarke Smith-Meyer, "EU countries revolt against Commission's dirty money list," *Politico*, 4 March 2019, https://www.politico.eu/article/eu-countries-revolt-against-commission-dirty-money-list-vera-jourova/

[8] "Anti-money laundering: Q & A on the EU list of high-risk third countries," European Commission, 13 February 2019, http://europa.eu/rapid/press-release_MEMO-19-782_en.htm

[9] Bjarke Smith-Meyer, "EU adopts tax haven blacklist," *Politico*, 12 March 2019, https://www.politico.eu/article/eu-adopts-tax-haven-blacklist-despite-romanian-doubts/

PARADIS FISCAUX, enfer de la fuite des capitaux du continent africain

« Paradis fiscaux, enfer des peuples africains » titrait en avril 2016, en plein scandale des Panama Papers, le journal burkinabé *le Pays*.

La définition même de paradis fiscal laisse à débattre. La notion même de « fiscalité » dans ce contexte, et prise isolément, n'a de sens que si elle peut être associée à ce que des spécialistes reconnus tels que Christian Chavagneux, Eric Vernier ou Gabriel Zucman qualifient de paradis bancaires, ou encore de paradis judiciaires. En effet, l'aspect fiscal de ces territoires constitue pour les criminels une variable moins importante que la recherche du laxisme réglementaire et de l'opacité. Les listes officielles même de paradis fiscaux laissent perplexes par l'objectivité de leurs contenus (telles que la liste française, européenne, de l'OCDE ou encore du GAFI). En effet, ces dernières rassemblent de petits territoires isolés, sans poids politique, et ce tout en laissant aux abonnés absents des pays puissants que l'ONG Tax Justice Network ou Nicholas Shaxson placent en tête de liste (les Etats Unis, la Suisse, Hong-Kong, le Royaume Uni ou encore le Luxembourg). Cependant et nonobstant tout cela, tout le monde s'accorde sur une chose : les paradis fiscaux, bancaires et judiciaires, quand on les nomme et lorsqu'ils sont utilisés illégalement pour couvrir la criminalité financière, sont un fléau pour la justice sociale. Ils sont en effet un fléau pour les pays développés mais encore plus pour les pays en voie de développement, et notamment, ici, pour le développement du continent africain.

« Les pays en développement ont perdu jusqu'à 1000 milliards de dollars en flux de capitaux illicites, soit dix dollars pour chaque dollars reçu au titre de l'aide étrangère »

Comme le notait Masimba Tafirenyika dans son article publié 2013 « Finance : ces capitaux qui fuient l'Afrique », entre 1980 et 2009, entre 1200 et 1400 milliards de dollars ont fui le continent africain, soit approximativement le PIB du continent dans son entier. Nicholas Shaxon faisait dans son œuvre un parallèle stupéfiant, notant que *« rien qu'en 2006, les pays en développement ont perdu jusqu'à 1000 milliards de dollars en flux de capitaux illicites, soit dix dollars pour chaque dollars reçu au titre de l'aide étrangère ».*

L'ONG CCFD Terre Solidaire estimait qu'avec les richesses qui quittaient illégalement les pays du Sud (comprenant ainsi notamment le continent africain), la faim dans le monde pouvait être éradiquée cinq fois. Une somme qui aurait également pu servir à l'éducation, la construction de routes, à l'amélioration du système sanitaire, à l'indépendance alimentaire, à la lutte contre la pauvreté ou à l'amélioration de l'ensemble des infrastructures publiques.

Une majeure partie de cette somme s'échappant des frontières africaines est le fruit d'actes illicites, voire criminels, d'une partie de l'élite africaine. Une somme issue des fruits de la corruption, de la fraude fiscale de la contrebande, du détournement de fonds et de richesses publiques. Comme le note Transparence Internationale via son célèbre classement annuel TI CPI, de nombreux pays d'Afrique, souvent parmi les plus pauvres de la planète, sont également parmi les plus corrompus au monde. Un cercle vicieux.

Les richesses se voient ainsi accaparées par des élites (via la perception de pots de vin dans les marchés publiques, le détournement de fonds publics, et de divers actes de corruption). Comme tout fonds illicites, ces derniers doivent être blanchis. Ainsi, les fonds illicites sont à la recherche de territoires complaisants pour être blanchis notamment en occident dans des secteurs attractifs tels que l'immobilier et les secteurs du luxe (en France comme nous avons pu l'observer avec l'affaire des Biens Mal Acquis, mais aussi à Londres, et aux Etats Unis). Ce processus n'est rendu possible que, d'une part, à l'aide de normes internes laxistes au niveau de la réglementation LCB/FT ou anticorruption africaine et, d'autre part, à l'aide de pays et territoires capables d'accueillir ces fonds criminels afin d'en masquer l'origine : les paradis fiscaux, bancaires et judiciaires. C'est ce que Nicolas Shaxson nomme les trois pointes du triangle (pays d'où fuient les capitaux : les pays d'Afrique qui constituent le placement des fonds, les centres offshores par où ils transitent qui favorisent l'empilement : que nous nommons ici les paradis fiscaux, bancaires et judiciaires, les pays qui les accueillent volontairement ou non : les pays occidentaux permettant l'intégration et la finalisation du processus de blanchiment).

Les paradis fiscaux, bancaires et judiciaires (Panama, Suisse, Lichtenstein, Luxembourg, territoires liés à la Couronne britanniques tels que les Iles Caïmans, Iles Vierges, ou encore les Etats Unis via des Etats tels que le Delaware ou la Floride) aident à, voire permettent directement de, masquer l'origine illicite des fonds qu'ils accueillent comme cela est à diverses

reprises pointé par les évaluations mutuelles menées par le GAFI. Constitution de Trust opaques, sociétés écran, actions au porteur, absence de vérification de l'identité du bénéficiaire effectif, services de prête noms, absence ou faiblesse dans les diligences menées sur l'origine des fonds et dans les normes KYC en général (dont la vérification de l'exposition politique du client final), absence de collaboration dans les enquêtes internationales ou encore, omniprésence d'un secret bancaire dont la violation est punie lourdement au pénal, sont monnaie courante au sein de ces territoires qui deviennent en finalité complices de ces actes.

Cette fuite, d'autres parleront de pillage, des ressources du continent a pu être étudiée en pratique à travers différents scandales planétaires véhiculés notamment par l'ICIJ (le consortium des journalistes d'investigations), et ce notamment en 2016 via les Panama Papers qui a permis au monde entier de se rendre compte de l'ampleur du phénomène. La plateforme « business-humanrights.org » pointait, en avril 2016 lors du leak, notamment la présence dans les listes de plusieurs dirigeants passés et présents africains qui, aidés par la firme spécialiste de l'offshore Mossak Fonseka, constituaient des sociétés écran offshore destinés à recevoir, en toute opacité, des fonds à l'origine douteuse quittant le continent : Adbeslam Bouchouareb, ministre de l'industrie et des mines d'Algérie, John Kufuor, ancien président du Ghana, Denis Sassou-Nguesso, président de la République Démocratique du Congo pour ne citer qu'eux.

Comme le notait en Marc Herkenrath dans Revue d'Economie du Développement (2014/2 vol 22, pages 151 à 156), les paradis fiscaux bancaires et judiciaires, en plus d'accueillir et de blanchir les fruits issus de la spoliation et de la corruption, établissent un cercle vicieux du phénomène en faussant les décisions d'investissements dans le continent et à contribuer à continuité de sa pauvreté malgré son potentiel énorme. En aidant les dirigeants corrompus et kleptocrates, les paradis fiscaux, bancaires et judiciaires aident ces mêmes personnes à continuer leurs activités illicites, à allouer les dépenses publiques et les appels d'offres vers des secteurs sensibles à la corruption (défense, extractions) pour pouvoir continuer de s'accaparer une partie des richesses et à entretenir le processus, tout en délaissant les secteurs clés au développement du pays (santé, éducation). C'est ce que notait en 2002 Tanzi et Davoodi dans ce même sens.

Des solutions ? Il y en a toujours, encore faut-il qu'il existe une réelle volonté internationale et locale. Fournir des aides financières au développement est une chose. En contrôler leur usage en est une autre. Cet argent devrait être octroyé pour doter les pays du continent de normes réglementaires de niveau comme le GAFI le préconise dans ses recommandations, et non pas sans contrepartie (ce qui tend à favoriser leur détournement). De normes anti-corruption adéquates également. La pédagogie plus que la sanction est ici de mise.

Ce qui sort d'un pays entre dans un autre. Il en va donc de même pour la nécessité de contrôler plus « sérieusement » les juridictions offshores, à la condition d'établir des listes « sérieuses » et non pas vides de sens. Nicholas Shaxson disait en page 36 de son livre sur les paradis fiscaux *« Personne n'est étonné quand je dis que le premier paradis fiscal de la*

planète est une île. En revanche, tout le monde est surpris quand je déclare que l'île en question s'appelle Manhattan. Quant au deuxième plus grand paradis fiscal, il aussi situé sur une île : c'est une ville du Royaume Uni nommée Londres. » L'exemple devrait donc également venir du Nord avant de se déverser vers le Sud. Cela demande cependant de revoir les priorités et délaisser les égoïsmes économiques au profit de plus de justice sociale.

Encadrer les utilisations parfois abusives de certaines structures et services (trusts, société écrans, actions au porteur, nominees) est essentiel également. Les normes du GAFI, solides sur le papier, le préconisent, mais les pays listés ne sont pas toujours les plus mauvais élèves dans les faits. Tout comme les directives européennes qui sont de plus en plus strictes, mais qui ne sont applicables qu'en Europe. Les écarts de conduite ne semblent que sanctionner, lorsqu'il y a sanctions, que des territoires sans appuis politiques (géopolitiques dirons-nous) ou économiques. Une homogénéisation est donc nécessaire, tout comme une indépendance entre volontés économiques souvent distantes des nécessités morales vis à vis de ces dernières.

Mais cela n'est pas irrémédiable comme le montrent plusieurs experts que nous avons ici cités. Ce n'est pas irrémédiable et l'avenir de l'Afrique en dépend.

Mustapha BOUZIZOUA, senior financial crimes compliance officer, HSBC Private Banking France, Paris, France, mustaphabouzizoua@yahoo.fr

Les nouveaux défis posés par la lutte anti-terroriste internationale

Avec l'assaut du village de Baghouz, près de la frontière entre la Syrie et l'Irak, l'État islamique[1] est en passe de perdre son dernier bastion territorial au Moyen-Orient.[2] Ainsi se terminera l'histoire récente tragique du contrôle territorial, dans la région, exercé par cette organisation terroriste. Toutefois, ceci met fin uniquement à la première étape de la lutte contre EI, car la guerre contre cette organisation n'est pas encore gagnée. Le groupe a réagi contre ses défaites militaires continues depuis 2016 en se réorganisant et se transformant, passant d'un groupe organisé en hiérarchie, soucieux de conquérir et de contrôler des territoires à un réseau fluide et clandestin de cellules terroristes, semblable à Al-Qaïda, avec une hiérarchie horizontale, qui se concentre sur les attaques terroristes.[3] Actuellement, cette transformation est plus avancée en Irak qu'en Syrie.[4] Sur le long terme, la question stratégique est encore de savoir si les deux réseaux terroristes internationaux que sont l'État islamique (EI) et Al-Qaïda ont l'intention de former une seule et même entité ou s'ils resteront deux organisations terroristes séparées.

De plus, cette transformation structurelle influe sur la façon dont l'EI réunit et dépense son argent. Avec la perte du contrôle territorial, l'EI a dû renoncer à la possibilité de générer des fonds grâce à l'exploitation systématique des ressources naturelles, au pillage des antiquités et à « l'imposition » de la population autochtone. Néanmoins, comme le groupe ne gère aucune grande ville ni aucune infrastructure, ses dépenses ont fortement baissé. En outre, le groupe continue d'avoir accès aux fonds sortis d'Irak et de Syrie depuis 2014 par l'intermédiaire de livreurs de fonds et de voies de paiement officieuses.[5] Les fonds disponibles pour l'EI sont estimés entre 50 et 300 millions de dollars américains.[6]

En agissant sous forme d'un réseau secret qui tente de susciter des attaques contre les personnes et cellules présentes dans la région et au-delà, les flux financiers vers et depuis le centre d l'EI en Irak et en Syrie seront probablement constitués de petits montants versés par des canaux de paiement ou des livreurs de fonds. Ceci complique le combat contre le financement du terrorisme. Par ailleurs, on s'attend à ce que les cellules de l'État islamique de la région et des alentours financent elles-mêmes leurs activités, ce qui réduira encore le besoin en flux de capitaux du groupe.[7] Toutefois, étant donné le volume considérable des fonds contrôlés par le groupe, l'EI doit trouver des moyens de les gérer et de dégager des ressources financières dans la zone de conflit. Le régime des sanctions contre le terrorisme international imposé par le Conseil de sécurité des Nations- unies (CSNU) constitue un instrument efficace contre ces menaces.

Modifications du régime des sanctions international pour combattre l'État Islamique

Suite aux attaques terroristes d'Al-Qaïda à Nairobi et Darussalam perpétrées en 1998, le Conseil de sécurité des Nations-unies a établi un régime de sanctions international visant le réseau d'Al-Qaïda et le régime des talibans en Afghanistan par le biais de la résolution 1267 (1999).[8] Le Conseil actualise continuellement ce programme de sanctions pour faire face à l'évolution des menaces. En réaction à l'émergence de l'EI, le Conseil de sécurité des Nations-unies (en collaboration avec le comité des sanctions et l'équipe de surveillance des talibans et de l'EI) a apporté d'importantes modifications à l'architecture des sanctions internationales. Depuis 2014, ces modifications visent à fournir des informations plus précises aux États membres des Nations-unies, ainsi qu'aux exécutants des sanctions du secteur privé, pour leur permettre de cibler plus spécifiquement les activités financières de l'EI et de contrer les nouvelles menaces que posent les combattants terroristes étrangers, les rapatriés et les combattants réaffectés.

Le Conseil a résolu le problème des combattants étrangers, réaffectés ou rapatriés en passant les résolutions 2178 (2014)[9] et 2368 (2017).[10] Dans ces résolutions, le Conseil a demandé aux États membres de criminaliser le déplacement des individus rejoignant

l'EI et de recueillir les informations préalables sur les voyageurs, ainsi que les noms des passagers de compagnies aériennes internationales, afin d'identifier les combattants étrangers, les rapatriés et les combattants réaffectés. Ceci a permis aux gouvernements d'identifier, de surveiller et d'intercepter plus souvent les terroristes en transit. Les résolutions 2199 (2015),[11] 2214 (2015)[12] et 2253 (2015)[13] ont permis au Conseil de sécurité de viser spécifiquement les activités de l'EI en Irak, en Syrie et en Libye, ainsi que le réseau international émergent de l'organisation. Non seulement ces résolutions ont ajouté l'EI et son commandement international à la liste existante des sanctions, mais elles ont également introduit de nouveaux aspects importants dans le régime des sanctions, par exemple l'exploitation des ressources naturelles comme le pétrole, et le pillage des antiquités auquel s'adonne l'EI. Par ailleurs, le Conseil de sécurité a voté plusieurs résolutions visant des formes particulières de comportement criminel dont use l'EI pour financer ses activités. La résolution 2347 (2017),[14] qui concernait la capacité de l'EI à générer des fonds grâce au pillage, au trafic et à la vente d'objets culturels, a établi une série de mesures permettant aux États membres et aux acteurs du secteur privé de se protéger contre l'abus du marché international des

L'usage abusif que fait l'EI des cryptomonnaies présente un nouveau défi

antiquités à des fins de financement du terrorisme.[15] Enfin, les Résolutions 2331 (2016)[16] et 2388 (2017)[17] visent à entraver les tentatives de l'EI d'obtenir des fonds au moyen du trafic humain.

En sus de ces modifications juridiques, le Conseil de sécurité a décidé d'actualiser la technologie utilisée pour dresser la « Liste des sanctions contre l'EI (Daech) et Al-Qaïda » afin de la rendre plus compatible avec les normes techniques actuelles des logiciels de compliance.[18] Cette mise à jour technique comprend l'introduction d'hyperliens dans les champs de données d'identification de la liste des sanctions, ce qui permet de relier les entrées des personnes physiques et morales respectives à la version publique des Notifications spéciales d'INTERPOL et du Conseil à leur sujet.[19] Ces notifications spéciales comprennent les photos et empreintes digitales de personnes sanctionnées, ce qui permet aux exécutants d'utiliser les données biométriques pour les reconnaître. Enfin, le Conseil de sécurité a demandé au Secrétaire général de signaler régulièrement et publiquement la menace changeante posée par l'EI, en sus des rapports publics de l'équipe de surveillance des talibans et d'Al-Qaïda.[20] Ces rapports, qui soulignent les principaux développements des tactiques terroristes employées par l'EI, y compris les tendances évolutives du financement de l'EI, peuvent servir à concevoir des typologies.

Défis émergents posés par le financement de l'EI

L'évolution actuelle du financement de l'EI présente quatre principaux défis à ceux qui luttent contre ses activités financières illicites : l'utilisation abusive des investissements illicites de l'EI et du secteur caritatif, l'extorsion, les voies de paiement officieuses ainsi que les cryptomonnaies.

À plusieurs reprises, il semble que l'EI ait blanchi des capitaux obtenus de manière illicite pour les réinvestir dans des sociétés nouvellement constituées dans la région : secteur agricole, immobilier, des bureaux de change, etc.[21] L'implication de l'EI dans certains secteurs de l'économie licite de la région nécessite potentiellement la mise en place d'une vigilance renforcée et de procédures de connaissance de la clientèle (KYC). Ce sera probablement un défi important à relever durant la reconstruction en cours en Irak et la reconstruction potentielle en Syrie.

Ceci est lié à une exploitation croissante du secteur caritatif par l'EI, non seulement pour transférer des fonds, mais aussi pour extorquer les partenaires locaux des programmes d'aide humanitaire. Ce n'est pas nouveau. Par le passé, Al-Qaïda exploitait régulièrement les organisations caritatives pour mener ses activités.[22] Toutefois, comme l'EI ne peut plus obtenir de financement par l'exploitation à grande échelle des ressources naturelles ni par « l'imposition » des populations autochtones sous son contrôle, on peut redouter une augmentation importante de l'extorsion des organisations caritatives ou des sociétés engagées dans la reconstruction.

Le rôle des voies de paiement officieuses pour financer le terrorisme est bien documenté.[23] Toutefois, les problèmes que présente l'inclusion financière dans les zones de conflit, telles que l'Irak, et les difficultés de transfert de fonds vers la Syrie (en raison des sanctions internationales contre le secteur financier syrien) augmentent les risques de transferts en espèces et de paiements officieux par l'EI en vue de dissimuler son financement, ses activités et ses transferts de fonds.

Enfin, l'usage abusif que fait l'EI des cryptomonnaies présente un nouveau défi. Depuis plusieurs années, déjà, les membres de l'EI manifestent un intérêt pour cette nouvelle technologie.[24] Jusqu'à ce jour, l'échange des cryptomonnaies contre des monnaies fiduciaires dans les zones de conflit, qui présente une difficulté pour l'EI, a limité son utilisation des cryptomonnaies pour lever ou transférer des fonds.[25] Toutefois, les cryptomonnaies, étant de nature internationale, deviennent de plus en plus accessibles. De plus, il est de plus en plus facile d'anonymiser l'identité des utilisateurs car, dans de nombreux États membres, la réglementation de cette technologie est inexistante ou commence seulement à apparaître. Ceci permet à l'EI de détourner cette technologie afin d'accumuler les fonds déjà en sa possession. Le projet Contre-extrémisme établit actuellement des recommandations réglementaires à cet égard.

En raison de ces défis, le combat contre le financement du terrorisme continuera effectivement de dépendre de diverses méthodes. Ce sont, entre autres, l'adaptation constante des typologies, les informations sur l'identité des financiers et facilitateurs du terrorisme, la cartographie des flux financiers et la réglementation efficace des nouvelles technologies pour garantir une transparence adéquate. Dans tous ces aspects, le régime des sanctions en matière de terrorisme du Conseil de sécurité continuera de jouer un rôle crucial, non seulement pour les organismes responsables du développement des contremesures des États membres, mais aussi pour les exécutants du secteur privé. La connaissance des informations fournies par le régime des sanctions, ainsi que le développement et le renforcement de partenariats efficaces entre organisations privées et publiques au sein des États membres, constituent des éléments cruciaux dans le combat contre l'évolution des activités financières de l'EI. A

Dr. Hans-Jakob SCHINDLER, directeur principal, Projet Contre-extrémisme, New York, États-Unis et Berlin, Allemagne, et ancien coordinateur de l'équipe de surveillance de l'EI, d'Al-Qaïda et des talibans, Conseil de sécurité des Nations-unies, hjschindler@counterextremism.com

[1] Included under reference number QDe.115 "Al-Qaida in Iraq" as AKA p) "Islamic State in Iraq and the Levant" (ISIL) by the United Nations Security Council in its global ISIL (Da'esh) & Al-Qaida Sanctions List.

[2] Ben Wedeman and Jay Croft, "Heavy fighting reported as US-backed forces attack last ISIS stronghold in Syria," CNN, 11 March 2019, https://www.cnn.com/2019/03/10/middleeast/syria-isis-stronghold-sdf/index.html

[3] "Third report of the Secretary-General on the threat posed by ISIL (Da'eash) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat," United Nations Security Council, 30 September 2016, http://undocs.org/S/2016/830

[4] "Letter dated 15 January 2019 from the Chair of the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'eash), Al-Qaida and associated individuals, groups, undertakings and entities address to the President of the Security Council," United Nations Security Council, 15 January 2019,http://undocs.org/S/2019/50

[5] Howard J. Shatz, "To Defeat the Islamic State, Follow the Money," RAND Corporation, 10 September 2014, https://www.rand.org/blog/2014/09/to-defeat-the-islamic-state-follow-the-money.html

[6] "Letter dated 15 January 2019 from the Chair of the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'eash), Al-Qaida and associated individuals, groups, undertakings and entities address to the President of the Security Council," United Nations Security Council, 15 January 2019, http://undocs.org/S/2019/50

[7] "Eighth Report of the Secretary General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat," United Nations Security Council, 1 February 2019, para. 14, http://undocs.org/en/S/2019/103

[8] "Security Council pursuant to resolutions 1267 (1999) 1989 (2011) and 2253 (2015) concerning ISL (Da'esh) Al-Qaida and associated individuals groups undertakings and entities)," United Nations Security Council, https://www.un.org/securitycouncil/sanctions/1267

[9] "Resolution 2178 (2014)," United Nations Security Council, 24 September 2014, http://unscr.com/en/resolutions/doc/2178

[10] "Resolution 2368 (2017)," United Nations Security Council, 20 July 2017, http://unscr.com/en/resolutions/doc/2368

[11] "Resolution 2199 (2015)," United Nations Security Council, 12 February 2015, http://unscr.com/en/resolutions/doc/2199

[12] "Resolution 2214 (2015)," United Nations Security Council, 27 March 2015, http://unscr.com/en/resolutions/doc/2214

[13] "Resolution 2253 (2015)," United Nations Security Council, 17 December 2015, http://unscr.com/en/resolutions/doc/2253

[14] "Resolution 2357 (2017)," United Nations Security Council, 24 March 2017, http://unscr.com/en/resolutions/doc/2347

[15] Ibid. See in particular par. 17.

[16] "Resolution 2331 (2016)," United Nations Security Council, 20 December 2016, http://unscr.com/en/resolutions/doc/2331

[17] "Resolution 2388 (2017)," United Nations Security Council, http://unscr.com/en/resolutions/doc/2388

[18] "Resolution 2253 (2015)," United Nations Security Council, 17 December 2015, http://unscr.com/en/resolutions/doc/2253. See par. 48.

[19] "Sanctions List Materials," United Nations Security Council, https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list. Each list entry is accompanied by a narrative summary for reasons of listing that includes additional biographical information. These narrative summaries are available from "Narratives Summaries of Reasons for Listing," United Nations Security Council, https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list/summaries. The INTERPOL-United Nations Security Council Special Notices for individuals are available from "View UN Notices – Individuals," INTERPOL, https://www.interpol.int/en/How-we-work/Notices/View-UN-Notices-Individuals. The notices for entities are available from "View UN Notices - Entities," INTERPOL, https://www.interpol.int/en/How-we-work/Notices/View-UN-Notices-Entities.

[20] "Resolution 2253 (2015)," United Nations Security Council, 17 December 2015, http://unscr.com/en/resolutions/doc/2253; "Resolution 2368 (2017)," United Nations Security Council, 20 July 2017, http://unscr.com/en/resolutions/doc/2368

[21] "Letter dated 17 January 2018 from the Chair of the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011), and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'aesh), Al-Qaida and associated individuals, groups, undertakings and entities addressed to the President of the Security Council," United Nations Security Council, 26 January 2018, https://undocs.org/S/2018/14

[22] "Wafa Humanitarian Organisation" United Nations Security Council, https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list/summaries/entity/wafa-humanitarian-organisation

[23] "Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)," Financial Action Task Force, February 2015, http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-IS.pdf; and "Emerging Terrorist Financing Risks," Financial Action Task Force, October 2015, http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf

[24] Ankit Panda, "Cryptocurrencies and National Security," Council on Foreign Relations, 28 February 2018, https://www.cfr.org/backgrounder/cryptocurrencies-and-national-security

[25] Yahya Fanusie, "Survey of Terrorist Groups and Their Means of Financing," House Financial Services Committee Subcomittee on Terrorism and Illicit Finance, 7 September 2018, https://www.fdd.org/wp-content/uploads/2018/10/09-07-18-Yaya-Fanusie-Written-Testimony.pdf

FINTECH : AMI ou ENNEMI du crime anti-financier ?

Note de l'auteur : La discussion sur les « fintechs », dans cet article, se rapporte aux comptes bancaires numériques (par ex. Monzo) et autres services de portefeuilles électroniques (par ex. Apple Pay).

Les fintechs sont des comptes bancaires numériques et des services de portefeuilles numériques. Un nombre croissant d'acteurs numériques propose des comptes de paiement, des fonds monétaires ou des services de virement d'argent. Ce qui est nouveau, c'est que leur adoption par les utilisateurs finaux croît aussi rapidement.[1] Il ne se passe pas une semaine sans que les médias ne parlent de banques d'un nouveau type (ou « banques néo ») comme Monzo, Revolut ou N26, qui accueillent de plus en plus de clients.[2]

Pourtant, le nombre de clients que perdent les établissements bancaires traditionnels ne semble pas alarmant. Alors, que se passe-t-il ? Pourquoi n'observe-t-on pas un transfert pur et simple entre les banques traditionnelles et les fintechs ?

Les clients adoptent ces nouvelles plateformes et ces nouveaux systèmes de paiement sans quitter leur banque traditionnelle.[3]

La raison est simple ; la plupart d'entre nous pouvons imaginer des raisons, selon nos propres situations et comportements, pour lesquelles nous garderions un compte bancaire traditionnel tout en ayant un compte fintech. En effet, nombre de ceux qui décident d'adopter les services bancaires fintech ne ferment pas leurs comptes bancaires « traditionnels » mais, au lieu de cela, gardent les deux, pour différentes raisons. Par exemple, les utilisateurs ont parfois besoin d'alimenter leurs comptes fintech, utilisant ainsi simplement leurs comptes bancaires traditionnels comme moyen d'acheminer les fonds dans leurs comptes numériques. Ou bien alors, leur banque traditionnelle propose des services que les prestataires fintech ne peuvent pas encore fournir, par exemple des investissements, prêts, etc. Il se peut également que les utilisateurs ne fassent pas encore entièrement confiance à leur prestataire de comptes fintech. Au sein de l'Union européenne (l'UE), tant que le prestataire de comptes fintech n'a pas obtenu de réelle concession bancaire, les fonds déposés par les clients ne sont pas garantis par les systèmes de garantie de dépôts de l'UE,[4] qui protègent les économies des déposants en garantissant les sommes déposées à hauteur de 100 000 euros.

Au sein de l'Union européenne (l'UE), tant que le prestataire de comptes fintech n'a pas obtenu de réelle concession bancaire, les fonds déposés par les clients ne sont pas garantis par les systèmes de garantie de dépôts de l'UE

Les utilisateurs finaux citent aussi, comme raison d'adopter des comptes fintech, entre autres, la facilité d'utilisation, les prix concurrentiels et une meilleure qualité de service.[5]

Cependant, cette myriade de nouvelles alternatives qui permettent à tout un chacun d'ouvrir un compte fintech et de recevoir des paiements (en général par carte bancaire) en quelques minutes pourraient-elles faciliter les crimes financiers ?

Sensibilisation à l'utilisation des fintechs à des fins potentiellement criminelles

Combien de lecteurs ont déjà un compte fintech ? Les professionnels LAB pourraient s'intéresser à ces méthodes préjudiciables (parfois uniquement en apparence) d'enregistrement des clients, de collecte et de vérification d'identité et, en général, de connaissance de la clientèle (KYC), pour ces clients qui peuvent même avoir plusieurs comptes de nouveau type et/ou fintech. Quelles informations sont demandées lors de l'enregistrement d'un nouveau compte ?

Fondamentalement, ce sont les mêmes informations, quels que soient les prestataires : données personnelles confirmées par une pièce d'identité émise par un État, parfois simplement un numéro d'identité fiscale nationale sans aucun autre justificatif.

On peut pratiquement ouvrir autant de comptes qu'il y a de prestataires fintech capables de les accueillir (essentiellement, ils vous fournissent un numéro de compte bancaire international).

Quelle est la différence entre les banques et établissements bancaires habituels et les fintechs ?

L'ouverture d'un compte bancaire dans un pays où l'on ne réside pas et/ou on ne perçoit pas son salaire prend bien plus que quelques minutes.

En fait, dans la plupart des banques de l'UE, même pour les citoyens européens, les informations suivantes doivent être fournies quand on essaie d'ouvrir un compte bancaire dans un pays où l'on ne réside pas :

- Justificatif d'emploi (contrat de travail ou preuve de l'immatriculation de la société pour les travailleurs indépendants)
- Justificatif d'enregistrement (auprès des autorités locales) dans le pays
- Les informations et documents habituels (en général, une pièce d'identité et un justificatif de domicile)

Tentation pour les criminels d'abandonner le système bancaire traditionnel

Les titres récents des médias en attestent : les autorités exercent une forte pression sur les banques traditionnelles pour qu'elles renforcent leurs contrôles LAB.

Les acteurs émergents du secteur des paiements, même s'ils n'évoluent pas dans un domaine anarchique, car ils doivent posséder une concession (principalement une concession d'établissement de paiement ou de monnaie électronique), tirent toujours profit de la réglementation de l'UE (grâce au mécanisme de passeport) pour opérer dans n'importe quel pays de l'Espace économique européen, tout en étant surveillé dans un autre.

Cela complique donc la tâche des organismes de réglementation du pays d'origine et du pays hôte en ce qui concerne la surveillance de leurs activités au sein de l'UE, surtout sans contrôleur actif à l'échelle de l'UE. Les criminels financiers en sont conscients.

Par exemple, un criminel pourrait vouloir frauder le fisc de 100 000 euros de capitaux obtenus illégalement en ouvrant facilement un des comptes décrits précédemment. L'ouverture de 10 comptes auprès de 10 prestataires de comptes fintech différents, chacun possédant une concession dans différents pays de l'UE, prendrait au plus 5 à 10 minutes par compte avec un smartphone et une pièce d'identité. Donc, même si le fintech s'acquitte de ses obligations contre le blanchiment d'argent/le financement du terrorisme (LAB/FT), il y a de grandes chances que le criminel n'ait pas à présenter plus d'informations ni de documents s'il dépose jusqu'à 10 000 euros sur chacun de ces comptes.

Pour aller plus loin, imaginez que la somme que le criminel tente de frauder ne soit plus de 100 000 euros mais de 1 000 000 euros. Le criminel ouvrirait quand même 10 différents comptes auprès de fintechs, chacun d'entre eux possédant une concession dans différents pays européens, mais, au lieu de déposer 10 000 euros sur chaque compte, il déposerait 100 000 euros structurés en plusieurs petites sommes.

Espérons que cela alerterait les systèmes de surveillance des fintechs. Il se peut même que le criminel soit invité à justifier l'origine des fonds avec des documents supplémentaires. Par ailleurs, les équipes LAB de fintechs peuvent même remplir et déposer un rapport d'activité suspecte (SAR) auprès de leur service de renseignements financiers local (FIU), mais alors que se passerait-il ?

Dix différents FIU situés dans 10 pays de l'UE différents peuvent être informés indépendamment qu'une personne effectue des dépôts structurés sur un compte fintech autorisé (par ex., types de licences : PI, EMI, banque spécialisée) dans leur pays.

Étant donné la charge de travail actuelle des FIU en Europe, il est très peu probable qu'une enquête plus poussée soit demandée suite à ce renseignement, s'il n'y a aucun lien avec d'autres incidents dans d'autres pays européens.

Par ailleurs, les FIU locaux de l'UE ne peuvent toujours pas se tourner vers un FIU de l'UE qui centraliserait les informations envoyées par tous les États membres.

Les risques de crime financier que posent ces fintechs/banques de nouveau type sont donc évidents, car il est très facile d'ouvrir plusieurs comptes en quelques minutes, n'importe où en Europe.

Actifs virtuels : incertitude juridique au profit des criminels

Imaginez que les prestataires de comptes fintech concernés soient, pour la plupart, des entités réglementées et, en tant que telles, doivent respecter les exigences LAB/FT de la même manière que les établissements bancaires normaux. Ce n'est pas encore le cas partout dans l'UE pour les fournisseurs d'actifs virtuels (bourses, prestataires de portefeuilles, etc.). En conséquence, les mesures suivantes, envisagées pour les prestataires fintech, ne sont pas nécessairement appliquées par ces acteurs :

- KYC / Vigilance à l'égard de la clientèle
- Surveillance LAB/FT des transactions
- SAR

Toutefois, heureusement, les principaux prestataires d'actifs virtuels les appliquent déjà. Non pas parce qu'il s'agit de « gens bien », mais parce que, sans ces mesures, ils n'auraient pratiquement aucune chance de travailler avec les établissements financiers avec lesquels ils collaborent (banques d'acquisition, banques commerciales, etc.) pour permettre leurs activités.

Quelles sont les solutions possibles pour neutraliser cette nouvelle menace ?

Du point de vue des autorités

Malgré les versions successives des directives de l'UE sur le LAB (car il existe encore de nombreuses différences entre les États membres en termes de réglementations LAB/FT et leur mise en œuvre) le système de passeport UE pourrait en fait affaiblir les mesures générales LAB/FT.

Afin de limiter le risque de circulation d'argent sale par l'intermédiaire d'acteurs de paiement en ligne, qui ne sont pas toujours très vigilants ni suffisamment contrôlés, les autorités de l'UE pourraient renforcer les pouvoirs des contrôleurs nationaux. En outre, la création d'un organisme de surveillance commun à toute l'UE faciliterait la transition d'un cadre réglementaire quelque peu normalisé vers une politique de répression peut-être plus normalisée.

Du point de vue des fintechs

Comme indiqué précédemment, les comptes fintechs sont généralement utilisés en tant que compte complémentaire plutôt que comme compte principal. Les modèles de surveillance et les alertes peuvent être conçus en conséquence.

Par exemple, on sait que la plupart des clients alimentent leurs comptes fintech depuis leurs comptes bancaires normaux, puis utilisent le solde pour effectuer des virements directs, par application mobile, à leurs amis ou à leur famille. Il est donc logique de poser des questions sur ceux qui reçoivent des fonds uniquement à partir de comptes qui ne leur appartiennent pas (fonds qu'ils transfèrent directement sur d'autres comptes), mais n'utilisent les produits fintech que pour cela.

Conclusion

Les prestataires de comptes fintech (les fintechs) et les systèmes de paiement émergents sont fascinants, car ils démystifient les produits financiers, facilitent la concurrence dans l'écosystème des services financiers (qui n'existait pas auparavant) et, en fin de compte, remettent les clients au centre de la prestation de services.

Néanmoins, technologie, innovation et perturbation ne doivent pas nous faire oublier que ces acteurs émergents ne sont pas encore habitués à la « culture de compliance » ni à opérer dans des environnements réglementaires en évolution permanente.

Ainsi, alors que nous découvrons régulièrement de nouvelles faiblesses et défaillances au sein des établissements bancaires établis de longue date dans l'UE, n'oublions pas que ces nouveaux venus, aussi positifs et bien intentionnés soient-ils, doivent aussi être étroitement surveillés. A

Alexandre PINOT, CAMS, chef du bureau de Vilnius et MLRO, SONECT Europe, Vilnius, Lituanie, alexandre@sonect.ch

La création d'un organisme de surveillance commun à toute l'UE faciliterait la transition d'un cadre réglementaire quelque peu normalisé vers une politique de répression peut-être plus normalisée

[1] "EY FinTech Adoption Index 2017: The rapid emergence of FinTech," EY, 2017, https://www.ey.com/Publication/vwLUAssets/ey-fintech-adoption-index-2017/$FILE/ey-fintech-adoption-index-2017.pdf

[2] "Neo and Challenger Bank Customer Base to Grow by 50.6%, Globally, by 2020," Allied Market Research, https://www.alliedmarketresearch.com/press-release/neo-and-challenger-bank-market.html

[3] Oliver Smith, "A Million U.K. Consumers Just Switched Their Bank Accounts—But Not To Fintech Challengers" Forbes, 26 July 2018, https://www.forbes.com/sites/oliversmith/2018/07/26/a-million-u-k-consumers-switched-their-bank-accounts-but-not-to-fintech-challengers/#462ca05f1205

[4] "Deposit guarantee schemes," European Commission, https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/managing-risks-banks-and-financial-institutions/deposit-guarantee-schemes_en

[5] Jeff Desjardins, "How Fintech is Digitally Disrupting the Financial World," Visual Capitalist, 3 August 2016, https://www.visualcapitalist.com/how-fintech-digitally-disrupting-financial-world/

Liaisons dangereuses : 5AMLD et EDD

La cinquième Directive anti-blanchiment de l'Union européenne (5AMLD),[1] entrée en vigueur le 9 juillet 2018, devra être mise en œuvre par les États membres d'ici janvier 2020. Les entreprises affectées par cette nouvelle directive, les entités concernées, sont confrontées à de nouveaux défis en raison des modifications pertinentes de la quatrième directive anti-blanchiment de l'UE (4AMLD) de 2015 (mise en œuvre en 2017).[2]

Les relations commerciales avec les pays tiers à haut risque, pays dont, d'après la Commission européenne, le système de financement de la lutte contre le blanchiment/le terrorisme [LAB/FT] présente de graves défaillances, sont particulièrement préoccupantes.[3] Cette nouvelle directive, qui exige une vigilance renforcée (EDD), suggère d'éventuelles restrictions commerciales envers ces pays à haut risque (voir l'encadré 2). Toutefois, la sélection des pays à inclure dans la liste noire s'avère controversée d'un point de vue politique (voir l'encadré 1).

Les institutions financières et autres entités concernées doivent comprendre qu'une liste noire de pays, établie suite à des négociations politiques, est inévitablement partiale et ne représente pas nécessairement une image complète de la réalité. Toute liste de l'UE ou autre liste similaire, dont celle du GAFI, devrait être complétée par une évaluation des risques des pays où sont implantées les entreprises, ainsi que par des articles de presse et des expertises fiables concernant les défaillances en matière de LAB. Ceci est également valable pour toute association avec des paradis fiscaux, cités dans une différente liste sélective de l'UE.

Cet article expose quelques-unes des autres modifications contenues dans la 5AMLD, qui entraînent de notables conséquences quant à la mise en œuvre de la vigilance fondée sur le risque à l'égard de la clientèle (CDD).

ENCADRÉ 1

Mesures de vigilance renforcée à l'égard des pays tiers à haut risque

L'Article 18a (Dir. 2018/843) exige la mise en œuvre de mesures EDD, dont l'obtention d'informations supplémentaires sur le client et les bénéficiaires effectifs ; la nature prévue de la relation commerciale ; l'origine des fonds et du patrimoine, et les motifs des transactions prévues ou effectuées.

Une mesure préventive particulière peut exiger que « le premier paiement soit effectué par l'intermédiaire d'un compte ouvert au nom du client, auprès d'un établissement de crédit soumis à des normes de vigilance à l'égard de la clientèle non moins strictes que les normes établies dans la présente directive ».

En sus des mesures renforcées d'atténuation et de surveillance des relations concernant les transactions effectuées avec des pays à haut risque, cette réglementation suggère de limiter les relations commerciales, par exemple par le « refus de l'établissement de filiales, succursales ou bureaux de liaison d'entreprises issues d'un pays tiers à haut risque », et « l'interdiction d'établir des filiales, succursales ou bureaux de liaison dans un pays concerné ».

Une autre clause stipule que « les relations de correspondant avec les institutions en question dans un pays à haut risque doivent être examinées et, le cas échéant, résiliées ».

ENCADRÉ 2

Liste controversée des pays tiers à haut risque

D'après l'Article 9 (2) de la Directive 2018/843, le 13 février 2019, la Commission européenne a présenté une liste de 23 pays à haut risque dont les stratégies LAB/FT présentent d'importantes défaillances.[4] Cette liste, qui dépasse le champ de la liste des « territoires surveillés à haut risque » du GAFI, comprenait 11 territoires supplémentaires, dont l'Arabie saoudite, le Panama et trois territoires américains : le Porto Rico, les Samoa américaines et les Îles Vierges des États-Unis. Le Trésor américain a critiqué cette liste.[5] En outre, cette liste a suscité des critiques pour avoir omis un nombre de pays considérés comme des cas évidents.[6] Qui plus est, cette liste n'a pas reçu l'agrément du Conseil européen qui lui a opposé son veto le 5 mars 2019.[7] Officiellement, le Conseil l'a rejetée pour des raisons de méthodologie, bien que la Commission ait expliqué dans sa proposition (C(2019)1326) la raison de sa sélection et indiqué qu'elle avait apparemment consulté les pays concernés avant de les inclure dans cette liste.[8]

Les différends concernant la liste des pays à haut risque sont contraires à l'esprit d'origine, celui d'une démarche harmonisée envers les pays à haut risque, en privilégiant les mesures d'atténuation et EDD standard, dans la mesure du possible. Dans tous les cas, la Commission, qui révise actuellement cette liste, devra obtenir l'accord du Conseil européen et du Parlement européen le plus tôt possible, pour éviter de se retrouver avec une liste édulcorée, ce qui nuirait à la crédibilité du processus tout entier.

Le 12 mars 2019, les ministres des Finances de l'UE ont adopté une liste révisée des pays considérés comme des paradis fiscaux, dont les Samoa américains, le Bahreïn, Aruba, la Barbade, Belize, les Bermudes, la Dominique, Fidji, Guam, les Îles Marshall, Oman, Samoa, Trinité-et-Tobago, les Îles Vierges des États-Unis, les Émirats arabes unis et Vanuatu.[9] Il reste à établir si la liste peut être considérée comme complète et significative, ou si elle a été raccourcie à des fins politiques. Bien sûr, la liste omet gracieusement les États membres de l'UE posant des problèmes d'administration fiscale.

Centralisation des informations sur la propriété

La 5AMLD entraîne des améliorations réglementaires afin de faciliter la première étape de toute procédure CDD, c'est-à-dire l'établissement du bénéficiaire effectif d'une entité concernée. À l'avenir, les registres des propriétaires bénéficiaires des États membres de l'UE seront plus centralisés, enrichis et plus facilement accessibles au public. Cela signifie que les registres devront être reliés par le biais de la plateforme centrale européenne prévue d'ici mars 2021. Il sera obligatoire de consulter cette plateforme avant d'établir de nouvelles relations d'affaires. Les fiducies et autres structures similaires seront incluses dans la plateforme commune des registres de propriétaires bénéficiaires. Au contraire de la pratique actuelle de certains États membres, le public pourra consulter les informations sur les propriétaires (en respectant certaines restrictions concernant les fiducies), permettant notamment à la presse et aux organisations de la société civile d'examiner ces données en détail.

Si l'UE réussit effectivement à mettre en place une plateforme de base de données centralisée contenant des informations fiables sur les propriétaire bénéficiaires, l'effet pourrait aller au-delà d'une meilleure recherche KYC (connaissance de la clientèle) ; elle ferait notamment passer le message que tout pays ne donnant pas accès à ces informations sur les propriétaires devrait être considéré comme un pays à haut risque sur le plan réglementaire. Concrètement, cela signifierait que, en cas d'entrave à toute recherche KYC sur les propriétaires bénéficiaires à l'aide des registres publics, des mesures EDD basées sur le risque, ou même le niveau suivant de vigilance en termes d'intégrité (IDD), y compris une enquête nationale approfondie, pourraient être déclenchées.

La lutte contre le blanchiment d'argent repose sur une interaction stratégique ; en effet, une réglementation plus stricte incitera probablement les auteurs potentiels à être plus inventifs plutôt qu'à abandonner. Ainsi, les bénéficiaires effectifs souhaitant vivre dans la clandestinité pourront soit se servir de territoires qui ne donnent pas d'informations sur les propriétaires, soit se dissimuler derrière des structures d'actionnariat complexes et stratifiées. Dans tous les cas, à l'avenir, les structures opaques empêchant d'identifier les propriétaires effectifs augmenteront encore l'exposition au risque.

À l'avenir, les registres des propriétaires bénéficiaires des États membres de l'UE seront plus centralisés, enrichis et plus facilement accessibles au public

Transparence du financement

En outre, le nouvel article 10 (1) de la 5AMLD exige que les États membres interdisent aux établissements de crédit et aux institutions financières de garantir l'anonymat des comptes, livrets ou coffres ; leurs propriétaires et bénéficiaires sont donc soumis aux mesures CDD (en vigueur depuis le 10 janvier 2019). Par ailleurs, un système automatique centralisé sera établi pour permettre d'identifier les titulaires de comptes de paiement et bancaires, ainsi que les coffres, d'ici septembre 2020. Ces informations seront à la disposition des services de renseignement financier et des organismes nationaux.

Concrètement, l'abolition des comptes anonymes permettra d'établir l'origine des fonds d'un client. Lors de l'établissement de relations d'affaires, l'origine des fonds doit toujours être transparente. En ce qui concerne les pays tiers, s'il n'est pas possible, en raison de l'anonymat ou autre obstacle, de découvrir la source du financement, un facteur de haut risque de ce type devrait déclencher une EDD pour étendre la portée de l'enquête sur la source du patrimoine général du client.

Concrètement, pour détecter si les fonds proviennent d'un produit illicite et/ou sont transférés dans le cadre d'un blanchiment d'argent, le flux des fonds doit être évalué dans le contexte des relations d'affaires et en fonction de l'objectif de la transaction. Tout soupçon portant sur l'utilisation d'intermédiaires (derrière lesquels les bénéficiaires effectifs des fonds potentiellement illicites peuvent se cacher) doit servir d'alerte et déclencher une EDD ou IDD.

Personnes exposées pour des raisons politiques

De plus, la 5AMLD permet des améliorations de la procédure CDD relative à l'identification des personnes exposées pour des raisons politiques. Les États membres doivent dresser une liste de fonctions ou de postes (et non pas de noms) spécifiques représentant les fonctions publiques importantes dans chaque pays, y compris ceux

d'organisations internationales enregistrées. Il reste à voir dans quelle mesure ces listes classeront les PPE différemment, par exemple à l'égard des dirigeants de parti ou maires de grandes villes. Dans tous les cas, l'identification d'une PPE, d'un parent ou d'un associé proche d'une PPE impliqué dans une relation avec les clients devrait être incluse dans les procédures de vigilance simplifiée, afin de déclencher des mesures EDD si ce critère de haut risque s'avérait pertinent.

L'utilisation des listes PPE préparées constitue un point de départ nécessaire, mais ne suffit probablement pas pour découvrir les liens indirects mais essentiels avec les PPE par l'intermédiaire de leurs associés. Qui plus est, de plus en plus de PPE réelles sauront qu'elles ont été repérées et celles qui ont quelque chose à cacher tenteront d'utiliser des intermédiaires afin d'éviter le déclenchement d'une alerte.

L'EDD effectuée à l'égard d'une PPE implique l'obtention d'informations supplémentaires pour savoir s'il est justifié de la qualifier de haut risque (par exemple en prouvant les intérêts commerciaux en question, toute utilisation douteuse d'un pouvoir, tout lien avec des activités irrégulières, voire corrompues), ce qui augmente le risque de l'implication dans des activités de blanchiment de capitaux. La définition de PPE est une définition fonctionnelle qui doit être prise en compte dans le contexte du territoire spécifique et de la relation commerciale. Le seuil utilisé pour qualifier de PPE une personne ayant des fonctions politiques devrait être revu à la baisse plutôt qu'à la hausse, afin d'exercer la vigilance adéquate et de détecter toute corruption ou tout blanchiment d'argent, le cas échéant.

Conclusion

La 5AMLD relève le niveau de vigilance renforcée à l'égard des clients à haut risque. Alors que l'UE se heurte à des difficultés politiques lorsqu'il s'agit de définir les territoires à haut risque à des fins LAB/FT et fiscales, la discussion controversée au sujet des listes de pays pertinents a fourni aux établissements financiers et autres sociétés concernées suffisamment de renseignements sur les pays à risque, difficiles à ignorer en exerçant une vigilance adéquate à l'égard des clients liés à ces pays. Quant à la vérification des informations client, la 5AMLD transmet clairement le message selon lequel l'acceptation d'une relation commerciale sans savoir qui est le bénéficiaire effectif ni la provenance des fonds entraîne de graves risques d'être associé à des criminels et à leurs produits illicites. Une vigilance renforcée devrait examiner les structures complexes de propriété, ainsi que les intermédiaires impliqués dans les mouvements des fonds. De même, l'identification de la participation anonyme d'une PPE à une propriété ou à des transactions nécessite une connaissance approfondie de l'environnement politique et commercial du client.

Dr. Carsten GIERSCH, associé principal, Berlin Risk Ltd., Berlin, Allemagne, carsten.giersch@berlinrisk.com

[1] "Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU," EUR-Lex, 30 May 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843

[2] "Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC," EUR-Lex, 20 May 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849

[3] "EU Policy on High-Risk Third Countries," European Commission, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/anti-money-laundering-and-counter-terrorist-financing/eu-policy-high-risk-third-countries_en; "EU Methodology for Identifying High-Risk Third Countries," Global Risk Affairs, 11 July 2018, https://www.globalriskaffairs.com/2018/07/eu-methodology-for-identifying-high-risk-third-countries/

[4] "Commission Delegated Regulation (EU) of 13.2.2019 supplementing Directive (EU) 2015/840 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies," European Commission, 13 February 2019, https://ec.europa.eu/info/sites/info/files/commission-delegated-regulation_hrtc.pdf

[5] "Treasury Statement on European Commission List of Jurisdictions with Strategic AML/CFT Deficiencies," U.S. Department of the Treasury, 13 February 2019, https://home.treasury.gov/news/press-releases/sm610

[6] "European Commission shames Saudi Arabia, Panama with 'dirty money' blacklist," International Consortium of Investigative Journalists, 14 February 2019, https://www.icij.org/blog/2019/02/european-commission-shames-saudi-arabia-panama-with-money-laundering-and-terror-financing-blacklist-but-attracts-criticism/

[7] Council of the European Union, 6964/1/19 REV 1; Bjarke Smith-Meyer, "EU countries revolt against Commission's dirty money list," *Politico*, 4 March 2019, https://www.politico.eu/article/eu-countries-revolt-against-commission-dirty-money-list-vera-jourova/

[8] "Anti-money laundering: Q & A on the EU list of high-risk third countries," European Commission, 13 February 2019, http://europa.eu/rapid/press-release_MEMO-19-782_en.htm

[9] Bjarke Smith-Meyer, "EU adopts tax haven blacklist," *Politico*, 12 March 2019, https://www.politico.eu/article/eu-adopts-tax-haven-blacklist-despite-romanian-doubts/

ACAMS® | Chapters

- Grow your professional network
- Attend exclusive events
- Hear from industry leaders
- Stay current on regional developments

Join your local chapter...or start a new one in your country!

Find out more at www.acams.org/chapters

NEW PODCAST SERIES

FINANCIAL CRIME MATTERS

WITH KIERAN BEER

LISTEN ON Spotify

Listen on Apple Podcasts

"I love when a podcast feels more like a living room conversation and you certainly achieved that.

I was so excited to see that there is FINALLY a financial crimes podcast.

In times like these, understanding the nature of financial crimes feels critical to understanding our world. This podcast is fascinating!"

ACAMS®

www.acams.org/podcasts