Client Alert | Financial Institutions Advisory / White Collar/Investigations / Data, Privacy & Cybersecurity

AML Information Sharing in a Technology-Enabled and Privacy-Conscious World

January 2019

Authors: **Kevin Petrasic**, **Paul Saltzman**, **Jonah Anderson**, **Jeremy Kuester**, **John Wagner**, **Rebecca Copcutt**, **John Timmons**

Financial firms play an integral role in preventing, identifying, investigating and reporting criminal activity, including terrorist financing, money laundering, and many other finance-related crimes. It is a critical role that depends on financial firms having the information they need to identify and report potentially suspicious activity and provide other relevant information to law enforcement. However, there are significant barriers to information sharing throughout the US anti-money laundering ("AML") regime. These barriers limit the effectiveness of AML information sharing within a financial institution, among financial institutions, and between financial institutions and law enforcement.

Much has changed in the 17 years following the passage of the USA PATRIOT Act ("**Patriot Act**"), which, among other things, sought to enable greater information sharing among law enforcement, regulators and financial institutions regarding AML risks. Of note, Section 314(a) of the Patriot Act and its implementing regulations ("**Section 314(a)**") enables federal, state, local and European Union law enforcement agencies to reach out to US financial institutions through the US Treasury Department's Financial Crimes Enforcement Network ("**FinCEN**") to locate accounts and transactions of persons that may be involved in terrorism or money laundering. Section 314(b) of the Patriot Act and its implementing regulations ("**Section 314(b)**") provides a limited safe harbor for financial institutions to share information with one another in order to better identify and report potential money laundering or terrorist activities.

While it is debatable whether Section 314(a) and Section 314(b) have achieved their desired potential, these programs represent an influential policy approach among various government attempts to improve the quality and depth of AML risk management within the financial services industry. The programs have inspired other attempts to drive AML information sharing among financial institutions and between government and industry, such as the creation of the United Kingdom's Joint Money Laundering Intelligence Taskforce in 2015 and the Criminal Finances Act of 2017, as well as similar approaches in Australia,[1] Singapore,[2]

Financial Institutions Advisory

- Bank Regulation, compliance and risk management
- Financial services digital transformation, including AI and RegTech
- Payments
- AML/BSA
- Blockchain and digital assets
- Regulatory and supervisory remediation, investigations and enforcement
- Bank recovery, restructuring, and resolution
- Marketplace and online lending
- Capital and liquidity regulation
- Consumer financial services
- Banking board and senior management governance
- Market Infrastructure, financial market utilities and CCPs

Hong Kong,[3] and Canada.[4]

At the same time, advances in technology and data science are also changing the way we think about AML information sharing and the protection of privacy interests. In this environment of changing and re-thinking, policymakers and regulators should ensure that the AML framework is clear and flexible to allow space for new technologies to flourish while protecting customer privacy and other core policy goals.

Barriers to AML Information Sharing

SAR Confidentiality

Enterprise-wide AML risk management remains a challenge, especially for multinational financial institutions. Under FinCEN rules,[5] a US financial institution may not share a suspicious activity report ("**SAR**"), or information that reveals the existence of such a report ("**SAR information**"), with third parties, including its non-US affiliates. While the SAR confidentiality rules are not intended to limit the sharing of underlying facts and transactions that led to the filing of a SAR, the prohibition on sharing "information that reveals the existence of such a report" leaves many financial institutions uncertain about the extent to which facts, descriptions of transactions, and documents that underlie a SAR (or even documents referenced in a SAR), may be shared.

The resulting uncertainty surrounding the extent to which a financial institution may share information with its non-US affiliates dampens the open exchange of AML information across an enterprise and may reduce a multinational financial institution's ability to detect suspicious activity across geographic regions and product lines. A less restrictive approach to the sharing of SARs and SAR information within an enterprise would likely improve overall AML risk management, including through more accurate transaction monitoring, higher quality SARs, and easier implementation of a risk-based, enterprise-wide approach to AML risk management.

FinCEN appears to recognize that confusion over the limits of SAR confidentiality may constitute a barrier to robust information sharing and that greater enterprise-wide sharing may be desirable. FinCEN now appears receptive to considering requests for exceptive relief from the SAR confidentiality rules on a case-by-case basis, although this is a relatively recent development. US financial institutions receiving such relief would be permitted to share SAR information with certain foreign affiliates, *provided that* the risks of disclosing the existence of a SAR are otherwise mitigated.

Privacy Requirements Applicable to the US Financial Sector

In the United States, financial institutions must comply with the Right to Financial Privacy Act, the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act and, potentially, state privacy laws, all of which govern what customer information institutions may share with affiliates, government entities and other third parties. Many such laws include carve-outs to relieve financial institutions of certain obligations when engaging in required information sharing under the Bank Secrecy Act ("**BSA**"). In addition, Section 314(b) provides a safe harbor from liability under such laws for the sharing of information in compliance with the Section 314(b) program.

These statutory carve-outs and safe harbors, which apply to specific instances of AML information sharing, offer a balance against some of the privacy law requirements that would otherwise limit or prohibit such sharing. Unfortunately, innovators seeking to re-think and improve AML information sharing often find that the protections provided by such carve-outs and safe harbors are not sufficiently flexible to shield innovators from potential liability under privacy laws. For example, financial institutions in the United States, the Netherlands and France, among others, are engaged in various initiatives to develop information-sharing utilities to exploit advances in machine learning and artificial intelligence to leverage the diverse sets of data maintained by different financial institutions. These utilities hold promise for dramatically improving the accuracy and efficiency of transaction and account monitoring and screening tools. However, existing information-sharing mechanisms, such as Section 314(b), may not be sufficiently broad to protect the institutions participating in such a utility from potential liability under the various privacy laws applicable to the financial sector.

European Data Protection and Privacy

Further complications arise from the application of the European Union General Data Protection Regulation ("**GDPR**") to financial institutions subject to AML reporting requirements. Generally speaking, a financial institution based outside of the European Union will be subject to the GDPR if it targets products and services

to European Union customers. The GDPR requires that organizations meet certain minimum requirements for the collection and sharing of personal information. For example, it may be permissible to share personal information for suspicious activity reporting or transaction reporting for AML purposes *provided that* notice was given to affected individuals when the information was originally collated and the financial institution has identified an appropriate "*legal basis*" under the GDPR.[6] If an organization shares personal information subject to the GDPR to comply with a legal obligation, this is only permissible if the legal obligation stems from the law of a country in the European Union. It is worth noting that, under direction from the National Crime Agency, members of the regulated sector in the UK can voluntarily share information between themselves for suspicious activity reporting without falling foul of data protection laws in the so-called "joint" or "super SAR" regime implemented under the Proceeds of Crime Act 2002, as amended by the Criminal Finances Act 2017.[7] However, the provisions of the GDPR relevant to data sharing are interpreted narrowly and so financial institutions must take care to comply with the necessary requirements when participating in AML information-sharing regimes that are built on voluntary sharing, such as the Section 314(b) program or the UK regime. Moreover, the Section 314(b) safe harbor specifically guards from potential liability under US laws and does not explicitly extend to potential liability under non-US laws, such as the GDPR. Financial institutions operating internationally must carefully analyze the risks before sharing personal information subject to European data protection laws with other financial institutions, even when sharing pursuant to programs such as Section 314(b) that permit voluntary AML information sharing among financial institutions.[8]

Technology-Enabled Solutions for More Effective Information Sharing

Technological Developments

Technology and data science innovations are creating intriguing possibilities for sharing AML information. These developments have the promise of making AML programs more effective and efficient through enhanced information sharing, as well as, in some cases, the potential to address certain of the privacy concerns traditionally associated with AML information sharing. Notable developments include the following:

- **Distributed ledger technologies**: Some governments are already exploring the use of distributed ledger technologies, including "smart contracts," to develop more efficient mechanisms by which financial institutions can fulfill regulatory reporting requirements.[9] Similar applications of distributed ledger technologies could be used to further simplify financial sector responses to requests for information from the government under Section 314(a), while in turn creating opportunities for the government to share otherwise sensitive information with the financial institutions that are in the best position to act upon it. Smart contracts could also be used to automate routine Section 314(b) exchanges, which are often valuable to the originator of the exchange request but time-consuming and resource-intensive for the respondent.

- **Machine learning**: Machine-learning technologies have the potential to make the transaction and account monitoring programs of financial institutions more powerful and accurate. Because the effectiveness of machine-learning technologies are in part a function of the quality and quantity of data available for analysis, these technologies are encouraging a re-thinking of the types of information that can and should be shared among financial institutions. As one example, permitting financial institutions to share "pre-suspicion" account and transaction information (*i.e.*, information that has not yet given rise to suspicion on the part of the sharing financial institution) would have the effect of creating bigger and more diverse pools of data from which the transaction-monitoring algorithms can "learn." Further, with the input and expertise of compliance officers across multiple institutions overseeing and validating the results of the algorithm, the mechanism would be likely to produce more accurate results, helping to reduce the false positive burdens that are common to existing account and transaction-monitoring systems. Both the US banking regulators and the UK's Financial Conduct Authority recently reported that they were seeing a large number of firms starting to explore machine learning.[10]

- **Privacy-enhancing technology**: Leveraging technology solutions may also be an effective strategy for managing privacy interests, while enabling robust and meaningful AML information sharing. For example, tools for converting sensitive customer information into anonymous or pseudonymous attributes are becoming more widely available. "Open algorithms" or "traveling algorithms," which are sent to and operate on existing data sets behind an institution's firewall and then share only encrypted results, are an intriguing advancement that could prevent the need to create centralized, shared data sets among financial institutions. Similarly, multi-party computation creates opportunities to generate utility-wide

values, such as identifying potentially suspicious activity across multiple institutions, without compromising the sensitive data of any individual financial institution.

Policies to Facilitate Technology Solutions

As exciting as these innovations are, they cannot flourish in a vacuum. It is critical that regulators and policymakers responsible for the AML framework keep pace with external events and ensure that AML policies, as well as related privacy policies, are sufficiently clear and flexible to support responsible innovations. The UK's Financial Conduct Authority, for example, is alert to its role in supporting the private sector through technological advancements. In July 2017, it commissioned a report about how new technologies are being used to streamline AML compliance[11] and its last annual report stated that it was exploring how technology can help firms comply with their obligations to detect and prevent money laundering.[12] US banking regulators also recently issued a joint statement encouraging banks and credit unions to take innovative approaches to combating money laundering, terrorist financing, and other illicit financial threats.[13]

To enable the creative use of technologies, particularly in regards to AML information sharing, regulators should ensure that their policies are clear and consistent and that there is agreement throughout the industry on the application of those policies.

For example, financial institutions' ability to facilitate and improve Section 314(b) exchanges using distributed ledger technologies and smart contracts is reliant on regulators establishing clear parameters for Section 341(b) programs. Unfortunately, the parameters for such exchanges remain unclear for many potential participants, with confusion existing as to when a financial institution may share information under Section 314(b). The most common source of confusion is in regards to what constitutes "possible terrorist or money laundering activities," a key predicate to Section 314(b) information sharing. Many institutions question whether they can share information only where there is a suspicion of explicit terrorist or money laundering activities, or whether they can instead share information when there is a suspicion of a predicate offense to money-laundering, such as fraud or other illegal conduct. FinCEN attempted to clarify this in a 2009 guidance,[14] which explained that the federal criminal money laundering statutes (18 U.S.C. §§ 1956 and 1957) include an array of predicate criminal activities, and if a financial institution suspects that a transaction involves the proceeds of one of those specified unlawful activities, it can presume that there would also be a reasonable suspicion of possible money-laundering and take advantage of the safe harbor. In a 2012 published administrative ruling interpreting aspects of the Section 314(b) program, FinCEN expanded upon this analysis, stating, "…FinCEN does not consider the sharing of information solely for the purpose of identifying a specified unlawful activity, including fraud, and not otherwise related to a transaction regarding the proceeds of such fraud, to be protected under the 314(b) safe harbor."[15] In the context of this guidance and ruling, it is difficult to understand how the sharing of information regarding a specified unlawful activity to another financial institution, which would be processing that information through its own accounts and transactions, would then not be able to impute a money-laundering nexus, as implied in the 2009 guidance. The two pronouncements from FinCEN can be read as contradictory and have created considerable confusion among financial institutions.

In addition, and as discussed above, unlocking the full potential of machine-learning technologies for the purposes of transaction- and account-monitoring programs requires robust data sets. Many financial institutions believe that permitting the sharing of "pre-suspicion" account and transaction information would be helpful in permitting the creation of such data sets. However, this type of expansive approach to AML information sharing to leverage technological gains might require national authorities to reconsider their policies on information-sharing safe harbors and the protection of consumer information.

Conclusion

Information-sharing challenges have long been an industry concern and have been flagged in extensive critiques of the BSA/AML regime.[16] Recent and ongoing technological developments provide an opportunity to move past those critiques and re-think AML information sharing in the context of a new operating environment. New considerations and tools will allow us to better address consumer privacy interests, while ensuring that governments have access to high-quality intelligence that allows them to combat serious criminal conduct. Continued dialogue between innovators, financial services industry participants and AML regulators will be necessary to ensure that we harness new technologies to build creative, safe and effective solutions.[17]

AMERICAS

New York

Ian Cuillerier
Partner
T +1 212 819 8713
E icuillerier@whitecase.com

Glen Cuccinello
Counsel
T +1 212 819 8239
E glen.cuccinello@whitecase.com

Virginia Romano
Partner
T +1 212 819 8601
E virginia.romano@whitecase.com

Paul Saltzman
Partner
T +1 212 819 8258
E paul.saltzman@whitecase.com

Edward So
Partner
T +1 212 819 7006
E edward.so@whitecase.com

Duane Wall
Partner of Counsel
T +1 202 626 3599
E duane.wall@whitecase.com

Francis Zou
Partner
T +1 212 819 8733
E francis.zou@whitecase.com

Washington, DC

Steve Chabinsky
Partner
T +1 202 626 3587
E steven.chabinsky@whitecase.com

Nicole Erb
Partner
T +1 202 626 3694
E nicole.erb@whitecase.com

Shamita Etienne-Cummings
Partner
T +1 202 626 3695
E shamita.etienne@whitecase.com

Will Giles
Counsel
T +1 202 637 6281
E will.giles@whitecase.com

Jeremy Kuester
Counsel
T +1 202 637 6284
E jeremy.kuester@whitecase.com

Helen Lee
Counsel
T +202 626 6531
E helen.lee@whitecase.com

Kevin Petrasic
Partner
T +1 202 626 3671
E kevin.petrasic@whitecase.com

Benjamin Saul
Partner
T +1 202 626 3665
E benjamin.saul@whitecase.com

Pratin Vallabhaneni
Partner
T +1 202 626 3596
E prat.vallabhaneni@whitecase.com

EMEA

Berlin

Dr. Henning Berger
Partner
T +49 30 880911 540
E henning.berger@whitecase.com

Frankfurt

Dr. Dennis Heuer
Partner
T +49 69 29994 1576
E dennis.heuer@whitecase.com

Matthias Kasch
Partner
T +49 69 29994 1219
E matthias.kasch@whitecase.com

Hamburg

Dr. Carsten Loesing
Local Partner
T +49 40 35005 265
E carsten.loesing@whitecase.com

Helsinki

Tanja Törnkvist
Partner
T +358 9 228 64 351
E tanja.tornkvist@whitecase.com

Istanbul

Asli Basgoz
Partner
T +90 212 354 2013
E asli.basgoz@whitecase.com

London

Laura Durrant
Partner
T +44 20 7532 2225
E laura.durrant@whitecase.com

Patrick Sarch
Partner
T +44 20 7532 2286
E patrick.sarch@whitecase.com

Julia Smithers Excell
Partner
T +44 20 7532 2229
E julia.smithers.excell@whitecase.com

Gavin Weir
Partner
T +44 20 7532 2113
E gavin.weir@whitecase.com

Stuart Willey
Partner
T +44 20 7532 1508
E stuart.willey@whitecase.com

Ingrid York
Partner
T +44 20 7532 1441
E iyork@whitecase.com

Madrid

Yoko Takagi
Partner
T +34 91 7876 320
E yoko.takagi@whitecase.com

Milan

Iacopo Canino
Partner
T +39 02 00688 340
E iacopo.canino@whitecase.com

Paris

Grégoire Karila
Partner
T +33 1 5504 5840
E gregoire.karila@whitecase.com

Thomas Le Vert
Partner
T +33 1 5504 1567
E thomas.levert@whitecase.com

Jean-Pierre Picca
Partner
T +33 1 55 04 58 30
E jeanpierre.picca@whitecase.com

Stockholm

Carl Hugo Parment
Partner
T +46 8 50632 341
E carlhugo.parment@whitecase.com

Warsaw

Tomasz Ostrowski
Partner
T +48 22 5050 123
E tostrowski@whitecase.com

Marcin Studniarek
Partner
T +48 22 5050 132
E marcin.studniarek@whitecase.com

1 On March 3, 2017, AUSTRAC, the Australian financial intelligence unit, launched the Fintel Alliance, a private-public partnership to combat money laundering and terrorism financing. More information is available at http://www.austrac.gov.au/about-us/fintel-alliance.

2 On April 24, 2017, the Monetary Authority of Singapore and the Commercial Affairs Department of the Singapore Police Force launched the Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership ("ACIP"). ACIP is a public-private partnership designed to collaboratively identify, assess, and mitigate the key money laundering and terrorism finance risks facing Singapore. More information is available at https://abs.org.sg/industry-guidelines/aml-cft-industry-partnership.

3 On May 26, 2017, the Hong Kong government, along with the Hong Kong Association of Banks and a number of banks, launched a pilot project, called the Fraud and Money Laundering Intelligence Taskforce to enhance the detection, prevention, and disruption of serious financial crime and money laundering threats. More information is available at https://www.hkma.gov.hk/eng/key-information/press-releases/2017/20170526-3.shtml.

4 FINTRAC, Canada's financial intelligence unit, has created several operational public-private partnerships to more effectively identify and trace illicit finance networks, namely Project Protect on human trafficking, Project Chameleon on romance fraud, and Project Guardian on the tracking of illicit fentanyl. More information is available at http://www.fintrac-canafe.gc.ca/publications/ar/2018/1-eng.asp#s4.

5 For example, SAR confidentiality rules for banks can be found in 31 CFR 1020.320(e) and similar provisions exist for all other financial institutions with a SAR obligation.

6 As a precondition to processing personal data, organizations must identify an appropriate "legal basis." The available legal bases are outlined in Article 6 and Article 9 of the GDPR and include, "contractual necessity," "legal obligations," "substantial public interest" and "legitimate interests."

7 For more information, see White & Case client alert on the Super SAR regime: *The Making of a Super-SAR* available at: https://www.whitecase.com/publications/alert/making-super-sar-case-study.

8 A UK Home Office Circular warns regulated entities to consider privacy interests, including the requirements of the GDPR and the Data Protection Act 2018, even as new legislation allows the entities to share information for AML purposes. Home Office Circular: Criminal Finances Act 2017, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/679032/HO_Circular-_Sharing_of_information_within_the_regulated_sector_1.0.pdf.

9 For example, in November 2016, the UK's Financial Conduct Authority facilitated a tech sprint on potential solutions to improve the efficiency of regulatory reporting. More information is available at https://www.fca.org.uk/events/techsprints/unlocking-regulatory-reporting-techsprint.

10 Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, FinCEN, National Credit Union Administration, Office of the Comptroller of the Currency, *Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist* Financing (Dec. 3, 2018) available at https://www.fincen.gov/sites/default/files/2018-12/Joint%20Statement%20on%20Innovation%20Statement%20%28Final%2011-30-18%29_508.pdf. FCA, *Anti-money laundering Annual Report 2017/18* available at: https://www.fca.org.uk/publication/corporate/annual-report-2017-18-anti-money-laundering.pdf. See also a speech by Rob Gruppetta, Head of the Financial Crime Department at the FCA, delivered to the FinTech Innovation in AML and Digital ID regional event in London (Dec. 6, 2017) available at https://www.fca.org.uk/news/speeches/using-artificial-intelligence-keep-criminal-funds-out-financial-system.

11 PA Consulting Group, *New Technologies and Anti-Money Laundering Compliance: Financial Conduct Authority* (Mar. 30, 2017) available at https://www.fca.org.uk/publication/research/new-technologies-in-aml-final-report.pdf.

12 *See* above at 8.

13 *See* above at 10.

14 FinCEN, *Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act*, FIN-2009-G002 (Jun. 16, 2009), available at https://www.fincen.gov/sites/default/files/shared/fin-2009-g002.pdf.

15 FinCEN, *Administrative Ruling Regarding the Participation of Associations of Financial Institutions in the 314(b) Program*, FIN-2012-R006 (Jul. 25, 2012), available at https://www.fincen.gov/sites/default/files/shared/FIN-2012-R006.pdf.

16 *See, e.g.*, The Clearing House, *A New Paradigm: Redesigning the US AML/CFT Framework to Protect National Security and Aid Law Enforcement* (Feb. 2017), available at https://www.theclearinghouse.org/~/media/TCH/Documents/TCH%20WEEKLY/2017/20170216_TCH_Report_AML_CFT_Framework_Redesign.pdf.

17 For more thoughts on regulators' efforts to encourage innovation in AML programs, please see White & Case's *Agencies Encourage Banks to Innovate in BSA/AML Compliance* (Dec. 7, 2018), available at https://www.whitecase.com/publications/alert/agencies-encourage-banks-innovate-bsaaml-compliance.