THE GUIDE TO ANTI-MONEY LAUNDERING

FIRST EDITION

Editor
Sharon Cohen Levin

Published in the United Kingdom by Law Business Research Ltd
Holborn Gate, 330 High Holborn, London, WC1V 7QT, UK

www.globalinvestigationsreview.com

Enquiries concerning reproduction should be sent to: insight@globalinvestigationsreview.com.
Enquiries concerning editorial content should be directed to the Publisher –
david.samuels@lbresearch.com

ISBN 978-1-80449-255-0

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

Acknowledgements

The publisher acknowledges and thanks the following for their learned assistance throughout the preparation of this book:

Accuracy

Charles River Associates

FTI Consulting Inc

Herbert Smith Freehills

Latham & Watkins LLP

Morgan, Lewis & Bockius LLP

Morgan Lewis Stamford LLC

Orrick, Herrington & Sutcliffe LLP

Sullivan & Cromwell LLP

Venable LLP

Von Wobeser y Sierra, SC

Willkie Farr & Gallagher LLP

Wilmer Cutler Pickering Hale and Dorr LLP

Publisher's Note

The Guide to Anti-Money Laundering is published by Global Investigations Review (GIR) – the online home for everyone who specialises in investigating and resolving suspected corporate wrongdoing. We tell our readers everything they need to know about all that matters in their chosen professional niche.

Thanks to GIR's position at the heart of the investigations community, we often spot gaps in the literature. *The Guide to Anti-Money Laundering* is a good example. For, despite a greater effort than ever to prosecute and eliminate money laundering by targeting financial gatekeepers, there is still no systematic work tying together all the trends in the area. This guide addresses that.

Its title is a little misleading. In fact, it covers both sides of the coin – trends in both the enforcement of money laundering laws (comprising Part I) and the operation of anti-money laundering regimes and the exigencies of compliance (Part II). Incorporating all of that in the title would have made it a little long (and slightly alarming: '*A Guide to Money Laundering . . .*' sounds quite wrong).

The guide is part of GIR's steadily growing technical library. This began six years ago with the first appearance of the revered GIR *Practitioner's Guide to Global Investigations*. *The Practitioner's Guide* tracks the life cycle of any internal investigation, from discovery of a potential problem to its resolution, telling the reader what to do or think about at every stage. Since then, we have published a series of volumes that go into more detail than is possible in *The Practitioner's Guide* about some of the specifics, including guides to sanctions, enforcement of securities laws, compliance and monitorships. I urge you to get copies of them all (they are available free of charge as PDFs and e-books on our website - www.globalinvestigationsreview.com).

Last, I would like to thank our external editor, Sharon Cohen Levin, for helping to shape our lumpier initial vision, and all the authors and my colleagues for the elan with which they have brought the guide to life.

We hope you find the book enjoyable and useful. And we welcome all suggestions on how to make it better. Please write to us at insight@globalinvestigationsreview.com.

David Samuels
Publisher, GIR
August 2023

CHAPTER 8

Challenges for Global Financial Institutions under Conflicting Legal Regimes

Britt Mosman, Laura Jehl, David Mortlock and Josh Nelson[1]

Introduction

Global financial institutions are required to navigate various legal obligations in each jurisdiction in which they operate with respect to anti-money laundering (AML) requirements and data privacy considerations. This is especially challenging where the different regimes impose different, and sometimes conflicting, obligations. The convergence of AML requirements and data privacy considerations, in particular, raises a unique set of challenges for financial institutions and other financial intermediaries. On the one hand, the objective of AML regulations is to create transparency to combat illicit financial activities and to protect the integrity of the global financial system. On the other hand, privacy and data protection laws seek to restrict the disclosures and handling of personal financial information to prevent any unauthorised access, use or disclosure of such information.

This chapter discusses key differences among AML and data privacy regimes in the United States, the United Kingdom and the European Union, explores the existing legal disconnections between the AML and privacy regimes and offers recommendations to global financial institutions caught in the middle.

---

1 Britt Mosman, Laura Jehl and David Mortlock are partners and Josh Nelson is an associate at Willkie Farr & Gallagher LLP.

Differences among AML regulatory regimes

Regardless of the jurisdiction, each AML regime we discuss in this chapter shares the same fundamental goal of safeguarding the financial system from the abuses of financial crime, including money laundering, terrorist financing and other illicit financial transactions. These legal frameworks generally require financial institutions and others to develop, implement and maintain AML compliance programmes to prevent and deter the evolving strategies of money launderers and terrorists who attempt to gain access to the legitimate financial system. Regulated persons are also generally required to report suspicious customer activity.

Financial institutions operating in multiple jurisdictions should ensure their compliance processes adequately cover the AML-related requirements of each applicable jurisdiction, which is particularly difficult where there is divergence among the regimes. Three important areas of distinction to consider are the differences in scope with respect to which entities are covered by the regulatory requirements, what information must be collected and when reports must be submitted to the government. Although the United States, the United Kingdom and the European Union each employ information collection and reporting requirements on financial institutions to effectuate their AML regimes, the entities and individuals that are subject to those requirements vary. Moreover, the type of information collected and disclosed can also change based on the location. Ensuring that global compliance programmes take into account the nuances of each jurisdiction is essential.

Although this chapter focuses on AML and data privacy issues, we note that similar challenges exist for global companies in navigating various sanctions and export controls regimes. These challenges have become more pronounced in the wake of Russia's invasion of Ukraine, in which US sanctions and export controls imposed on Russia have not always been the most restrictive. Although the United States, the United Kingdom and the European Union have each implemented widespread sanctions and export controls measures in an effort to restrict Russian access to the global financial system, the programmes are not uniform and each reflects different priorities and policy objectives. Global financial institutions and other companies operating in multiple jurisdictions now must undertake analysis to determine which sanctions and export controls regimes are applicable to their activities and ensure that their compliance programmes are able to meet expectations for each.

Scope of covered financial institutions

The United States, the United Kingdom and the European Union each regulate financial institutions for AML purposes, but each jurisdiction defines the scope of regulated financial institutions differently and considers different sectors as participating in the financial system (as detailed below). For example, the United Kingdom and the European Union consider lawyers and legal notaries to be regulated for AML purposes, which is something that the American Bar Association has strongly opposed in the United States.[2] The European Union also regulates crypto service providers directly, whereas in the United States they are only regulated insofar as they qualify as a money services business.

United States

The Bank Secrecy Act, as amended (BSA), is the principal US federal statute aimed at preventing money laundering. Pursuant to the BSA and implementing regulations administered by the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), various types of financial institutions are required to comply with comprehensive AML-related requirements, including to implement and maintain risk-based AML compliance programmes that meet certain minimum standards.[3] Regulated financial institutions include:

- banks (except bank credit card systems);
- brokers or dealers in securities;
- money services businesses;
- telegraph companies;
- casinos;
- card clubs; and
- any person subject to supervision by any state or federal bank supervisory authority.[4]

Money services businesses are a broad subset of regulated financial institutions and include:

- dealers in foreign exchange;
- cheque cashers;

2 See 'Gatekeeper Regulations on Attorneys', American Bar Association (https://www.americanbar.org/advocacy/governmental_legislative_work/priorities_policy/independence_of_the_legal_profession/bank_secrecy_act/ (accessed 11 July 2023)).

3 31 U.S.C. § 5318(h)(1); 31 C.F.R. § 1010.200.

4 31 C.F.R. 1010.100(t).

- issuers or sellers of traveller's cheques or money orders;
- providers and sellers of prepaid access;
- money transmitters; and
- United States Postal Service.[5]

Significantly, various other entities that can play key roles in the US financial system currently fall outside the scope of the BSA framework, including registered investment advisers, private investment vehicles, certain third-party payment processers, art dealers and real estate professionals. The US government continues to assess the illicit finance risks related to other types of financial institutions that are not subject to comprehensive AML regulations to determine whether additional AML measures would be appropriate. For example, a 2015 Notice of Proposed Rulemaking by FinCEN proposed to subject registered investment advisers to AML requirements.[6]

United Kingdom

The primary pieces of AML legislation are the Financial Services and Markets Act 2000, the Proceeds of Crime Act 2002 and the Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017 (the 2017 Regulations). Many of the UK authorities are based on EU AML directives, although changes have been made under subsequent legislation.[7] Under these authorities, regulated financial institutions are required to implement AML programmes that collect information about customers and transactions, including beneficial ownership, and report suspicious transactions. AML regulations apply to:

- financial and credit businesses;
- independent legal professionals;
- accountants, tax advisers, auditors and insolvency practitioners;

---

5 31 C.F.R. 1010.100(ff).

6 See US Department of the Treasury, Financial Crimes Enforcement Network (FinCEN), 'Anti-Money Laundering Program and Suspicious Activity Report Filing Requirements for Registered Investment Advisers, Notice of Proposed Rulemaking' (80 Fed. Reg. 52,680), (1 September 2015) (https://www.federalregister.gov/documents/2015/09/01/2015-21318/anti-money-laundering-program-and-suspicious-activity-report-filing-requirements-for-registered (accessed 11 July 2023)).

7 The Money Laundering and Transfer of Funds (Information) (Amendment) (EU Exit) Regulations 2019, The Money Laundering and Terrorist Financing (Amendment) (EU Exit) Regulations 2020, The Money Laundering and Terrorist Financing (Amendment) Regulations 2022, and The Money Laundering and Terrorist Financing (Amendment) (No. 2) Regulations 2022.

- trust and company service providers;
- estate agency businesses;
- letting agency businesses;
- casinos;
- high value dealers;
- article market participants;
- cryptoasset exchange providers; and
- custodian wallet providers.[8]

Although the Financial Conduct Authority has primary responsibility for regulating AML in the financial services industry in the United Kingdom, all regulated entities are required to register with the supervisor that regulates their industry sector;[9] for example, casinos must register with the Gambling Commission.

European Union

AML standards across the European Union are set by directives established at the EU level that are implemented through national implementing legislation. The legislation and resulting jurisprudence must not deviate from EU rules; if it does, the directive prevails.[10] However, the exact wording and methods of interpretation may vary from country to country. In any event, the entities subject to AML regulation in the European Union are known as obliged entities and include:

- credit institutions;
- financial institutions;[11]

8 The Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017, Regulation 8.

9 https://www.gov.uk/anti-money-laundering-registration (accessed 11 July 2023).

10 See https://finance.ec.europa.eu/system/files/2022-03/aml-ctf-lawyers-training-trainers-manual_en.pdf (accessed 11 July 2023), pp. 9–10.

11 'Financial institutions' is broadly defined to include: (1) an undertaking other than a credit institution that carries out one or more of the activities listed in points (2) to (12), (14) and (15) of Annex I to Directive 2013/36/EU of the European Parliament and of the Council on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, including the activities of currency exchange offices (bureaux de change); (2) an insurance undertaking as defined in point (1) of Article 13 of Directive 2009/138/EC of the European Parliament and of the Council on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (recast), insofar as it carries out life assurance activities covered by that Directive; (3) an investment firm

- certain natural or legal persons acting in the exercise of their professional activities, including auditors, external accountants, tax advisers, notaries and other independent legal professionals engaged in certain activities;[12]
- trust or company service providers;
- estate agents, including when acting as intermediaries in the letting of immovable property for transactions for which the monthly rent amounts to €10,000 or more, or the equivalent in the national currency;
- persons trading in precious metals and stones;
- providers of gambling services; and
- cryptoasset service providers.

As much of the enforcement of AML regulations is left to EU Member States, currently there is no EU-wide AML regulatory authority. However, the Sixth Anti-Money Laundering Directive proposed the establishment of such an authority, which remains pending.[13]

---

as defined in point (1) of Article 4(1) of Directive 2004/39/EC of the European Parliament and of the Council on markets in financial instruments; (4) a collective investment undertaking marketing its units or shares; (5) an insurance intermediary as defined in point (5) of Article 2 of Directive 2002/92/EC of the European Parliament and of the Council on insurance mediation where it acts with respect to life insurance and other investment-related services, with the exception of a tied insurance intermediary as defined in point (7) of that Article; and (6) branches, when located in the European Union, of financial institutions as referred to in points (1) to (5), whether their head office is situated in a Member State or in a third country.

12 Such activities include participation, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or carrying out of transactions for their client concerning any of the following: buying and selling of real estate property or business entities; managing of client money, securities or other assets; opening or management of bank, savings or securities accounts; organisation of contributions necessary for the creation, operation or management of companies; creation, operation or management of trusts, companies, foundations, or similar structures. See 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 (4th EU Anti Money Laundering Directive (AMLD), Article 2.

13 See European Parliament, 'Anti-money-laundering authority (AMLA): Countering money laundering and the financing of terrorism' (15 May 2023) (https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733645 (accessed 11 July 2023)).

Information collected

One of the primary features of the AML requirements for financial institutions is the general requirement to collect and verify identification information from customers when opening an account and to conduct continuing customer due diligence periodically thereafter. However, there are subtle differences among the regimes regarding what exactly must be collected, and frequent updates to the requirements, so global financial institutions must stay informed about the differing requirements. Below we discuss key aspects of the regimes in the United States, the United Kingdom and the European Union.

United States

Regulated financial institutions in the United States are required to develop and implement a customer identification programme that establishes procedures for identifying and verifying the identity of each customer who opens a new account, so that the financial institution can form a reasonable belief that it knows the true identity of each customer.[14] As a minimum, financial institutions must obtain the name, date of birth (for natural persons), address and an identification number.[15] Further, financial institutions must collect information regarding the beneficial owners of legal entity customers at the time a new account is opened.[16] Certain regulated financial institutions are required to establish due diligence programmes that include specific, risk-based and, where necessary, enhanced procedures and controls reasonably designed to enable the financial institution to detect and report known or suspected money laundering conduct involving a foreign correspondent account.[17]

In addition, the 'Travel Rule' requires regulated financial institutions to pass specified information to the next financial institution in funds transmittals of more than US$3,000 involving more than one financial institution – whether in US dollars, virtual currencies or foreign currencies.[18] Necessary information includes the name, account number and address of the transmitter; the amount

14 31 C.F.R. § 1010.220(a).

15 id.

16 31 C.F.R. § 1010.230. Beginning on 1 January 2024, this requirement will be expanded through the establishment of beneficial ownership reporting under the Corporate Transparency Act, which will require corporations and other legal entities to directly report information about their beneficial owners to FinCEN. Further rule-making is expected to align the beneficial ownership requirements for financial institutions and other legal entities.

17 31 C.F.R. § 1010.610.

18 31 C.F.R. § 1010.410(f).

and execution date of the transmittal order; and the identities of the transmitter's and the recipient's financial institutions. Significantly, FinCEN has proposed lowering this threshold to US$250 for transactions that begin or end outside the United States.[19]

United Kingdom

Similarly to the United States, the United Kingdom requires financial institutions to identify their customers through customer due diligence (CDD) using a risk-based process. Firms must apply CDD measures when they establish business relationships, suspect money laundering or terrorist financing, carry out an occasional transaction or doubt someone's prior identification verification.[20] These requirements mirror EU AML requirements. CDD verification includes the identify of an individual and beneficial ownership information about individuals owning 25 per cent or more of a legal entity.[21]

CDD measures may be simplified or enhanced based on various risk factors as laid out in the 2017 Regulations (as amended), effectively creating a three-tiered approach.[22] Simplified CDD is permissible when a financial institution determines that the business relationship or transaction presents a low risk of money laundering or terrorist financing based on whether:

- the customer is a public administration or enterprise, a financial institution itself subject to AML regulation, an individual located in the United Kingdom or a third country with effective systems for AML and countering terrorist financing, or a company whose stock is traded on a regulated market;[23] or

19 FinCEN, Notice of Proposed Rule-making, 'Agency Information Collection Activities; Proposed Renewal; Comment Request; Renewal Without Change of Regulations Requiring Records to be Made and Retained by Financial Institutions, Banks, and Providers and Sellers of Prepaid Access' (23 December 2020) (https://www.federalregister.gov/documents/2020/12/23/2020-28364/agency-information-collection-activities-proposed-renewal-comment-request-renewal-without-change-of (accessed 11 July 2023)).

20 The Joint Money Laundering Steering Group, 'Prevention of money laundering/combating terrorist financing: Guidance for the UK Financial Sector' (hereinafter JMLSG), at 5.2 (https://www.jmlsg.org.uk/guidance/current-guidance/ (accessed 11 July 2023)).

21 JMLSG, at 5.3.

22 Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017 (2017 Regulations), Part 3.

23 2017 Regulations, Article 37, Paragraph 3.

- the product is considered low risk; for example, certain life insurance and pension schemes, a child trust fund, or a product where the risks of money laundering or terrorist financing are low because of the characteristics of the product (such as transparent ownership).[24]

If simplified CDD is permissible, the financial institution is not required to conduct the standard CDD procedures.[25] Conversely, enhanced CDD is necessary when circumstances relating to the transaction or the customer indicate a higher risk of money laundering or terrorist financing, such as:

- any business relationship with a person or a transaction concerning a third country identified as high risk;
- correspondent relationships with a credit institution or financial institution;
- if the customer or potential customer is a politically exposed person or a family member or close associate of a politically exposed person;
- if it is discovered that the customer has provided false or stolen identification documents and the financial institution continues to deal with the customer; and
- any other case where the financial institution determines there is a high risk of money laundering or terrorist financing based on the available information.[26]

If enhanced CDD is required under the circumstances of a transaction, the financial institution must obtain additional information about the customer (and their beneficial owner, if applicable), the intended nature of the business relationship, the source of funds and the customer's wealth, and the reason for the transaction.[27] Further, approval of the financial institution's senior management is required and the financial institution must conduct enhanced monitoring of the customer.[28]

The United Kingdom has an established registry, similar to the pending US beneficial ownership database, that records people with significant control (PSC) in entities.[29] PSC are individuals who control 25 per cent or more of the shares

24 id.

25 JMLSG, Annex 5-III.

26 2017 Regulations, at Article 33.

27 id.

28 id.

29 Economic Crime and Corporate Transparency Bill 2022, 'Factsheet: beneficial ownership' (https://www.gov.uk/government/publications/economic-crime-and-corporate-transparency-bill-2022-factsheets/factsheet-beneficial-ownership (accessed 11 July 2023)).

or voting rights in a company, hold the right to appoint the majority of the board of directors, or otherwise have the right to exercise significant influence over the company.[30] The PSC registry, established in 2016, requires UK companies and other legal entities to identify who owns and controls them with Companies House, a UK executive agency. Further, the Register of Overseas Entities, established in 2022 and the first of its kind, requires overseas entities that own UK property to identify their beneficial owners.[31]

Similar to the US Travel Rule, the United Kingdom requires that financial institutions transmit information about the payer and payee when transferring funds. The UK rules mirror the EU Funds Transfer Regulation,[32] which requires payment service providers to provide information about the payer (e.g., name, account number, address, identification number) and payee (e.g., name and account number).[33] Unlike the US Travel Rule, the United Kingdom does not have a threshold for when this information must be reported; it must be reported on all transactions.[34] This will be extended to crypto payments as of 23 September 2023 and will apply to transactions worth more than €1,000.[35]

European Union

Obliged entities must establish policies, controls and procedures to ensure compliance with EU AML law.[36] The European Union requires obliged entities to conduct CDD when establishing a relationship, conducting an occasional transaction, when there is a suspicion of money laundering or terrorist financing, or when there are doubts as to the veracity or adequacy of previously obtained customer identification data.[37] Like the United Kingdom, the European Union requires obliged entities to collect beneficial ownership information for legal entities, mirroring the 25 per cent requirement.

---

30 id.

31 id.

32 Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds.

33 Regulation (EU) 2015/847, Article 4.

34 See The Money Laundering and Transfer of Funds (Information) (Amendment) (EU Exit) Regulations 2019, Article 15(2)(d) (removing the €1,000 threshold discussed below).

35 See 'United Kingdom's Crypto Travel Rule To Start September 2023', Sygna (https://www.sygna.io/blog/united-kingdoms-crypto-travel-rule-to-start-september-2023/#:~:text=What%20Is%20the%20FATF%20Travel,cross%20the%20threshold%20of%20%241%2C000 (accessed 11 July 2023)).

36 4th AMLD, Article 45(1).

37 ibid., at Article 11(1).

EU Member States must establish beneficial ownership registries.[38] This information is collected in a central register, the Beneficial Ownership Registers Interconnection System (BORIS). Although individual national beneficial ownership registries are publicly available, the European Court of Justice held in November 2022 that BORIS cannot provide public access to the information held in national beneficial ownership registers.[39]

Similar to the United States and the United Kingdom, the European Union requires payment service providers to ensure that transfers of funds are accompanied by information about the payer (e.g., name, account number, address, identification number) and payee (e.g., name and account number).[40] Like the United Kingdom, the European Union does not set a threshold for when this information must be provided. However, Member States may choose to waive these information transfer requirements when the transfer is €1,000 or less.[41] The European Union is preparing an extension of its Travel Rule to crypto payments, which is expected to take effect in 2025.[42]

Reporting requirements

Reporting suspicious activity and transactions is the foundation of the AML reporting framework across regimes because of how critical it is to the regulators and law enforcement authorities that utilise the information reported to combat financial crimes. However, as detailed below, the structure and specific requirements of suspicious activity and transaction reporting varies; moreover, regimes differ with respect to other types of reports that are required.

38 4th AMLD, Article 31(3a) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02015L0849-20210630 (accessed 11 July 2023)).

39 European Court of Justice, C-37/20 and C-601/20; Beneficial Ownership Registers – search for beneficial ownership information (https://e-justice.europa.eu/38576/EN/beneficial_ownership_registers__search_for_beneficial_ownership_information (accessed 11 July 2023)).

40 Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds, Article 4(1).

41 ibid., at Article 2(5)(b).

42 See 'Crypto assets: deal on new rules to stop illicit flows in the EU', European Parliament (29 June 2022) (https://www.europarl.europa.eu/news/en/press-room/20220627IPR33919/crypto-assets-deal-on-new-rules-to-stop-illicit-flows-in-the-eu (accessed 11 July 2023)).

United States

All US financial institutions are required to file two principal types of reports with FinCEN – suspicious activity reports (SARs) and currency transaction reports (CTRs). The filing of these reports significantly contributes to the compliance burden that financial institutions face.

Banks and other financial institutions must file a SAR with FinCEN when financial institutions know or suspect violations of law or observe suspicious activity by a customer.[43] A suspicious transaction may involve funds derived from illegal activities, evasion of BSA requirements or has no apparent lawful purpose.[44] SARs are confidential and may not be disclosed to any person, including the subject of the SAR.[45] Other financial institutions are subject to the same SAR requirements, with an emphasis on the use of their services to facilitate criminal activity.[46]

All financial institutions other than casinos are required to file CTRs for transactions that involve the payment or transfer of more than US$10,000.[47] In connection with CTRs, financial institutions are required to record the name and address of the person presenting the transaction, among other personal information.[48] Evasion of CTRs through multiple transactions below the US$10,000 threshold is known as structuring and is expressly prohibited.[49]

Although financial institutions are required to file CTRs, all US persons must report receipt of more than US$10,000 in cash in one transaction.[50] Courts are required to make similar reports in connection with the receipt of bail.[51] The requirement that US persons report cash transactions at the same threshold as the requirement for financial institutions to file CTRs is designed to mitigate the risk that money launderers and terrorist financiers attempt to bypass AML reporting systems by transacting in cash.

---

43 See, e.g., 31 C.F.R. § 1020.320 (concerning suspicious activity report requirements for banks).

44 id.

45 31 C.F.R. § 1020.320(e).

46 See, e.g., 31 C.F.R. § 1022.320(a)(2)(iv), 31 C.F.R. § 1023.320(a)(2)(iv), 31 C.F.R. § 1024.320(a)(2)(iv) (each, concerning the use of the financial institution to facilitate criminal activity).

47 31 C.F.R. § 1010.311.

48 31 C.F.R. § 1010.312.

49 31 C.F.R. § 1010.314.

50 31 C.F.R. § 1010.330.

51 31 C.F.R. § 1010.331.

United Kingdom

Although the United Kingdom requires firms in the regulated sector to submit SARs, there is no equivalent to CTRs. SARs must be submitted to the National Crime Agency when a firm knows, suspects or has reasonable grounds to know or suspect that a transaction or other activity may be linked to money laundering or terrorist financing.[52] As with the United States, the United Kingdom prohibits disclosure that a SAR has been made, including to the subject of the report.[53]

European Union

Obliged entities shall report to their national financial intelligence unit all suspicious transactions in a suspicious transaction report (STR).[54] A transaction is considered suspicious where the obliged entity knows, suspects or has reasonable grounds to suspect that funds are the proceeds of criminal activity or related to terrorist financing. As in the United States and the United Kingdom, the existence of an STR shall not be disclosed to the person who is the subject of the report or any other third party.[55] However, like the United Kingdom, the European Union has no requirement that transactions over a certain threshold be automatically reported, as with the US CTRs.

Compliance conflicts

International financial institutions and others subject to multiple AML regimes should understand the differences between the programmes so as to ensure that their compliance programmes address each relevant jurisdiction. Activity that is reportable in one jurisdiction is not necessarily reportable in all jurisdictions, and some entities – such as law firms – may be required to enact AML programmes in Europe and the United Kingdom, but not the United States.

Recommendations for navigating multiple AML regimes

Although the AML laws and regulations of the United States, the United Kingdom and the European Union share many similarities, the differences discussed above (among others) mean that developing an AML compliance programme that is consistent with each regime is more complicated than it may seem at first. Given this complexity, some financial institutions with group companies in each regime

52 JMLSG, at 6.35.

53 Proceeds of Crime Act 2022, Section 333A.

54 4th AMLD at Article 33.

55 ibid., at Article 39.

choose to implement group-wide AML policies and procedures that apply the most restrictive regime globally, especially with respect to CDD-related issues and overall programme management. It is important to note, however, that local laws must still be followed when it comes to reporting and information sharing procedures, as well as the appropriateness of relying on another person to conduct any aspect of a regulated entity's regulatory requirements.

More generally, effective AML compliance programmes in each of these regimes will include:

- an AML risk assessment that is periodically reviewed and updated;
- development of written internal policies, procedures and controls;
- designation of an AML compliance officer;
- regular AML employee training;
- independent testing or auditing of the AML programme;
- appropriate risk-based procedures for conducting continuing CDD so as to understand the nature and purpose of customer relationships and to conduct continuing monitoring to identify and report suspicious transactions, and, consistent with the level of risk, to maintain and update customer information; and
- policies and procedures covering CDD, risk management, internal controls, reporting and record-keeping.

In addition, a financial institution's board of directors should provide sufficient oversight for senior management in the maintenance and enhancement of the AML compliance programme.

Conflicts between AML requirements and data privacy restrictions

The increasing digitisation of global financial services and transactions has intensified the threat associated with the potential unauthorised access to financial information. More than ever, individuals' financial information is at risk of being exposed and leveraged without their consent.

To address these concerns, financial institutions are subject to various restrictions on how they may collect, use and share personal information, to better safeguard the privacy and integrity of their customers' financial information. Conversely, as discussed in this chapter, financial institutions are also subjected to disclosure obligations for the financial information they collect in the context of reporting obligations under AML laws.

The convergence of AML requirements and data privacy restrictions raises a unique set of challenges for financial institutions and regulators. On the one hand, the objective of AML regulations is to create transparency to combat illicit financial activities and protect the integrity of the global financial system. On the other hand, privacy and data protection laws seek to restrict the disclosure and handling of personal financial information to prevent any unauthorised access, use or disclosure of such information.

Existing financial privacy restrictions

The requirements introduced by national AML regimes share greater symmetry at the international level than do national and regional privacy regimes – especially in the United States and the European Union – which take distinct approaches to privacy and protecting personal information. Although both jurisdictions recognise the importance of privacy, there are notable differences in their legal frameworks governing data protection.

In the United States, personal information is typically the property of the data holder. The US Constitution does not explicitly mention privacy but the Supreme Court has ruled that the Bill of Rights creates 'zones of privacy' within several Amendments, including the 1st (freedom of speech), 3rd (privacy of the home), 4th (protection of the person and possessions against unreasonable searches and seizures) and 5th (self-incrimination). In the European Union, privacy is a fundamental right, and personal information ownership is vested in the individual, regardless of the institution holding the data.

Furthermore, in the United States, privacy protection is primarily regulated at a sectoral level. The United States does not have a comprehensive federal privacy law comparable to the European Union's General Data Protection Regulation (EU GDPR).[56] Instead, the United States relies on a patchwork of industry, audience or data-specific federal privacy and data security laws and regulations (e.g., healthcare, banking and financial services, children and biometric data), as well as state privacy laws focused on consumer protection (e.g., the California Consumer Privacy Act). In contrast, the European Union takes a largely harmonised

56 Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and the free movement of such data (General Data Protection Regulation) (EU GDPR) (https://eur-lex.europa.eu/EN/legal-content/summary/general-data-protection-regulation-gdpr.html (accessed 11 July 2023)).

and comprehensive approach to regulating privacy with the EU GDPR at its centre. With very few exceptions, the EU GDPR applies uniformly across all 27 Members States and the countries in the European Economic Area (EEA) and sets out a strict framework for data collection, processing and transfer. When the United Kingdom withdrew from the European Union in 2020, the EU GDPR was incorporated into United Kingdom law as the UK GDPR.[57]

Financial privacy in the United States

Overview

Regulation of financial information in the United States is spread across a host of government entities[58] and gives financial institutions considerable control over the terms and services they provide, as well as over how they use customer data. Generally, the United States operates under an opt-out model, whereby an individual's personal information may be processed by a business unless the individual explicitly objects to the processing and informs the company. In addition, US financial institutions' requirements with respect to the privacy of financial information are generally limited to informing individuals of their rights and any changes to their policies and procedures. As a result, individuals have limited power over their financial information in the United States once they sign up for services, in contrast to the EU model which provides data ownership to the individual.

We now offer an overview of the key financial privacy laws in the United States, outlining their scope and purpose and the privacy obligations they impose on financial institutions.

57 The EU GDPR was transposed into United Kingdom law under the European Union (Withdrawal) Act 2018, as amended by the European Union (Withdrawal Agreement 2020), as set out in the United Kingdom Data Protection Act 2018 (UK GDPR).

58 The applicable regulatory authority depends on the financial institution at play but may include the Federal Trade Commission (FTC), Federal Reserve, Consumer Finance Protection Bureau, Office of the Comptroller of the Currency, Commodity Futures Trading Commission and Securities and Exchange Commission. The state attorneys general may also be involved.

Gramm-Leach-Bliley Act

Enacted in 1999, the Gramm-Leach-Bliley Act (GLBA) generally provides the general framework for the confidentiality of records in the financial sector.[59] The GLBA aims to safeguard consumers' personal information held by financial institutions. Under the GLBA, financial institutions are required to:

- provide customers with a notice explaining how they share and protect their personal information;
- offer customers the right to opt out of having their personal information shared with third parties; and
- refrain from disclosing their customers' personal information to any third-party marketer.

Along with privacy standards and rules, in 2003 the GLBA established additional security standards in the form of the Safeguard Rule, which requires certain security controls to protect the confidentiality and integrity of personal consumer information. Under the GLBA Safeguard Rule, financial institutions are required to design and implement specific information security policies and procedures to protect their customers' financial information against security threats and unauthorised access to, or certain uses of, such records or information. The programme must be appropriate for the size, complexity, nature and scope of the activities of the relevant institution.

Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA) was passed in 1970 to regulate the collection of and access to consumers' credit information and to address the fairness, accuracy and privacy of the personal information contained in credit report files.[60] The FCRA governs how consumer reporting agencies provide consumer reports, which are used to assist in establishing a consumer's eligibility for credit.[61] A consumer report may include information about a person's credit standing, creditworthiness, credit capacity, character, general reputation and mode of living. The FCRA defines the scope and obligations of users who are allowed to obtain a

---

59 Gramm-Leach-Bliley Act, 15 U.S.C., Subchapter I, Sections 6801 to 6809 (1999) (https://www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/documents/8/viii-1-1.pdf (accessed 11 July 2023)).

60 12 C.F.R. Part 1022 – Fair Credit Reporting (Regulation V), Consumer Financial Protection Bureau (https://www.consumerfinance.gov/rules-policy/regulations/1022/ (accessed 11 July 2023)).

61 id.

consumer report. Users include businesses, which may use the information in deciding whether to make a loan or sell insurance to a consumer, and employers making employment decisions, as long as they have a 'permissible purpose' under the FCRA to obtain a consumer report. Permissible purposes for obtaining a consumer report include:

- a court order;
- a written consumer request;
- employment purposes (e.g., hiring);
- underwriting of insurance pursuant to a consumer application;
- a legitimate business need in the context of a business transaction initiated by the consumer; or
- reviewing a consumer's account to determine whether the consumer meets the terms of the account.

Additionally, the FCRA provides consumers with certain rights over their consumer reports, including to:

- access and review the accuracy of the credit report;
- notice if information in their report has been used against them when applying for credit or other transactions;
- dispute and correct any information contained in their report that is incomplete or inaccurate; and
- remove outdated and damaging information after seven years for most cases or 10 years for some bankruptcies.

Fair and Accurate Credit Transactions Act

The Fair and Accurate Credit Transactions Act (FACTA) was passed by Congress in 2003 and made substantial amendments to the FCRA to include provisions on identity theft and other subjects.[62] In particular, FACTA enabled a number of consumer protections, such as the truncation of payment card information, so

62 16 C.F.R. Part 682 – Disposal of Consumer Report Information and Records (https://www.ecfr.gov/current/title-16/chapter-I/subchapter-F/part-682 (accessed 11 July 2023)); see 'The Fair Credit Reporting Act (FCRA) and the Privacy of Your Credit Report', Electronic Privacy Information Center (https://epic.org/fcra/ (accessed 11 July 2023)).

that receipts would not reveal the full numbers. FACTA also gave consumers new rights to obtain an explanation of their credit scores. Further, the Act established two major rules in the data processing of financial consumer information:

- The Disposal Rule set requirements for how financial institutions must destroy consumer reports to prevent any unauthorised access to non-public consumer information.[63]
- The Red Flags Rule requires financial institutions to develop and implement written identity theft detection programmes that can identify and respond to the red flags that signal identity theft.[64]

Right to Financial Privacy Act

The Right to Financial Privacy Act (RFRA) permits federal government authorities access to financial information only where the government has made a legitimate request pursuant to a valid court order.[65] The RFRA allows financial institutions to provide information upon government request if:

- the institution keeps appropriate records of a customer's financial records;
- the records are relevant to a legitimate law enforcement enquiry;
- the records are properly requested via an administrative subpoena, search warrant, judicial subpoena or formal written request; and
- the customer is given notice of the disclosure and an opportunity to object to the disclosure request.

Consumer Financial Protection Act (Dodd-Frank)

The Dodd-Frank Act was enacted in 2010 as a response to the 2008 financial crisis and, among numerous other reforms, created the Consumer Financial Protection Bureau (CFPB). The CFPB oversees the relationship between consumers and financial institutions and generally assumes rule-making authority for specific existing laws concerning financial privacy (e.g., the GLBA and the FCRA).[66]

---

63 'Disposing of Consumer Report Information? Rules Tell How', FTC (https://www.ftc.gov/business-guidance/resources/disposing-consumer-report-information-rule-tells-how (accessed 11 July 2023)).

64 16 C.F.R. Part 681 (https://www.ecfr.gov/current/title-16/chapter-I/subchapter-F/part-681 (accessed 11 July 2023)).

65 12 U.S.C. § 3402, et seq.

66 Dodd-Frank Wall Street Reform and Consumer Protection Act, 12 U.S.C. § 5512 (https://www.cftc.gov/sites/default/files/idc/groups/public/@swaps/documents/file/hr4173_enrolledbill.pdf (accessed 11 July 2023)).

Notably, the Dodd-Frank Act empowered the CFPB to enforce against 'abusive acts and practices', which had previously been a power reserved to the Federal Trade Commission and the state attorneys general. An abusive act or practice may include an act or practice that:

> *(1) materially interferes with the ability of a consumer to understand a term or condition of a consumer financial product or service; or*
> *(2) takes unreasonable advantage of—*
> *(A) a lack of understanding on the part of the consumer of the material risks, costs, or conditions of the product or service*[67]

For instance, the CFPB holds the power to bring enforcement actions for unfair or deceptive privacy policies and other aspects of privacy and security protection by financial institutions.

California Financial Information Privacy Act (CFIPA)

The California Financial Information Privacy Act (CFIPA) expands the financial privacy protections afforded under the GLBA for California consumers.[68] The CFIPA increases financial institutions' disclosure requirements and provides California consumers with additional rights with regard to the sharing of their personal information; for example, the CFIPA requires financial institutions to obtain written opt-in consent from consumers before sharing any personal information with non-affiliated third parties. Similarly, the CFIPA provides California consumers with the right to opt out of information sharing between their financial institutions and affiliates.

Financial privacy in the European Union and the United Kingdom

The EU GDPR was implemented in 2018 and is the cornerstone of European financial privacy laws. Both the EU GDPR and the UK GDPR set forth rules for data processing, storage, retention and record-keeping that apply to any businesses and organisations that perform operations on the personal information

67 ibid., at 12 U.S.C. § 5531.

68 California Financial Code, Section 4050 et seq.

of individuals living in the European Union, regardless of where the processing of the data takes place. Within the financial sector, these obligations have far-reaching implications, compelling financial institutions to ensure the utmost protection of their customers' financial information, transparency and accountability. These obligations include:

- *having a lawful basis for data processing*: under the EU GDPR and the UK GDPR, personal information 'shall be processed lawfully, fairly and in a transparent manner in relation to the data subject'.[69] Namely, personal information must be processed only if a legal ground exists. Acceptable legal grounds under the EU GDPR and the UK GDPR include consent, contractual performance, legal obligation, public interest, vital interest of individuals and legitimate interest;
- *transparency and providing privacy notices*: the EU GDPR and the UK GDPR places a significant emphasis on providing individuals with clear and easily understandable information regarding how their personal information is collected, processed and stored;[70]
- *purpose limitation*: under the EU GDPR and the UK GDPR, covered businesses must only collect and process personal information to accomplish a specific legal purpose and cannot process personal information beyond that purpose unless the further processing is considered compatible with the purpose for which the personal information was originally collected;[71]
- *data minimisation*: the principle of data minimisation establishes that a covered business must only collect and process personal information that is relevant, necessary and adequate to accomplish the purpose for which it is processed.[72] As a result, under the EU GDPR and the UK GDPR, businesses are required to carefully assess the necessity and proportionality of the personal information collected and limit it to what is directly relevant and necessary to accomplish a specified purpose;[73] and

69 ibid., at Article 5(1).

70 id.

71 ibid., at Article 5(1)(b).

72 ibid., at Article 6(1)(c).

73 Refer to Data Protection Glossary (https://edps.europa.eu/data-protection/data-protection/glossary/d_en (accessed 11 July 2023)).

- *establishing retention periods*: the EU GDPR and the UK GDPR establishes that personal information must not be kept for longer than necessary for the purpose for which the personal information is processed. In other words, once the information is no longer needed, it must be securely deleted.[74]

In addition to the EU GDPR, in 2020, the European Parliament adopted a revised version of the Payment Services Directive (PSD2).[75] The PSD2 regulates payment providers and sets rules for access to payment account information. The revised Directive aims to reduce fraud, improve customer choice and introduce new requirements for payment service providers while enhancing consumers' control over their financial data.[76] In particular, the revisions require that payment service providers obtain explicit customer consent for accessing and using their payment account information. Customers must be provided with clear information about how their data will be used and have the ability to grant or revoke their consent at any time.

Conflicting accountabilities: AML versus privacy

The legal disconnections between the US and EU financial privacy laws and the AML regimes present unique challenges to the ability of global financial institutions to implement consistent policies and procedures across their business and jurisdictions. These disconnections may also leave a gap for unauthorised data-gathering and illicit economy.

Notably, the rules and restrictions under the EU GDPR and the UK GDPR imposed on financial institutions conflict with AML regulations. The overarching effect of the EU GDPR and the UK GDPR is to regulate and, to a certain extent, limit the circumstances under which data can be processed. These requirements

74 General Data Protection Regulation (GDPR), Recital 39.

75 Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation No 1093/2010, and repealing Directive 2007/64/EC.

76 id.

raise an inherent risk of conflict between the EU GDPR and the UK GDPR and the AML regimes if they are not implemented in alignment. In particular, the following key issues call for careful consideration:

- *Retention of records*: AML requirements across jurisdictions generally require covered financial institutions to retain records to prevent, detect and investigate possible money laundering or terrorist financing after the end of the business relationship with a customer or after the date of an occasional transaction.[77] By contrast, the EU GDPR and the UK GDPR require that personal information not be kept longer than necessary and provides individuals with a right to erase their personal information (the right to be forgotten).[78] This dual standard creates complexities for global financial institutions when storing data for AML purposes.
- *Data sharing with third countries*. Owing to differing data protection standards and legal frameworks across jurisdictions, cross-border data transfers present significant challenges when reconciling privacy and AML compliance. The EU GDPR and the UK GDPR hold financial institutions accountable for any data transferred outside the EEA or the United Kingdom to a third country, stipulating that the data can only be shared with a recipient country that provides adequate data protection.[79] However, many countries are not considered adequate by the European Union and the United Kingdom. This situation creates a potential conflict for organisations operating in both the European Union and other jurisdictions when transferring personal information for AML purposes, as organisations must ensure compliance with both AML obligations and EU GDPR and UK GDPR transfer restrictions.

Moreover, the existing legal disconnections between the AML and privacy regimes also raise risks in the context of access to records by government authorities for AML purposes. Governments often emphasise the need for access to financial records and customer information to effectively combat money laundering and other financial crimes. Financial information is particularly interesting to states as it can help to track illicit economic flows and potentially dangerous networks, which causes financial information to exist as both commercial information and a source of intelligence for governments; however, this can conflict with individuals'

77 6th Money Laundering Directive, Article 40(1) (https://lexparency.org/eu/32015L0849/ART_40/ ()) (accessed 11 July 2023)).

78 GDPR, Recitals 30 and 53, Articles 17 and 18(2a).

79 GDPR, Recitals 78 and 83.

privacy rights and the principles of proportionality and necessity. Striking the right balance between national security imperatives and privacy considerations is a continuing challenge.

For instance, in the United States, law enforcement agencies may access financial information if they obtain a warrant under Fourth Amendment jurisprudence. Additionally, financial privacy protections are increasingly threatened by a growing commercial surveillance industry that involves the collection of vast amounts of purchase-level transactional and precise geolocation information that presents significant opportunities for commercial data brokers to leverage financial data in the absence of controlling privacy laws.[80] Much of this data is available for purchase from brokers by almost anyone, including law enforcement agencies with little oversight or protections against the circumventions of existing constitutional protections against illegal searches and seizures.[81]

80 In August 2022, the FTC announced it was exploring rules to crack down on data brokers and highlighted the risks stemming from commercial consumer surveillance and the absence of an adequate legal regime to control these practices. See press release, 'FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices' (11 August 2022) (https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices (accessed 11 July 2023)).

81 For example, US Immigrations and Customs Enforcement (ICE) was accused of purchasing from data brokers transaction data from utility payments to identify allegedly undocumented individuals for arrest and deportation. Some of the data used by ICE was collected by the credit reporting agency Equifax from another data broker holding more than 400 million utility records. See Georgetown Center on Privacy and Technology, American Dragnet, Data-Driven Deportation in the 21st Century (10 May 2022) (https://americandragnet.org/finding3 (accessed 11 July 2023)). See also Drew Harwell, 'ICE investigators used a private utility database covering millions to pursue immigration violations', *The Washington Post* (26 February 2021) (https://www.washingtonpost.com/technology/2021/02/26/ice-private-utility-data/ (accessed 11 July 2023)).