HIGHLIGHTS

- Central bank digital currencies (CBDCs) provide an unprecedented opportunity to design digital money that is inherently resistant to money laundering and the financing of terrorism.
- Strong forms of digital identity enable the customer due diligence process to be largely automated and make it challenging for bad actors to use a CBDC.
- Ongoing algorithmic transaction monitoring and interoperable record keeping approaches can enable collaboration between financial institutions to better identify criminal behavior while balancing privacy and financial inclusion.

This article explores how technical central bank digital currency (CBDC) design choices can be used to make a CBDC inherently resistant to money laundering. These design choices not only further anti-money laundering (AML), but they can also help to better balance AML priorities with other goals including financial inclusion, privacy and compliance costs. Moreover, CBDCs provide an opportunity to measure the effectiveness of different design choices in real time. These measurements can facilitate the iterative redesign of CBDCs to identify optimal approaches to meeting regulatory objectives.

CBDC and AML Overview

Defining CBDCs: At their core CBDCs are a liability of a central bank issued in digital form [3]. A retail CBDC is accessible to the general public, while a wholesale CBDC is limited to certain entities, generally financial institutions. CBDCs differ from stablecoins – cryptocurrencies that are pegged to an external currency – because they are issued by a government and thus carry all the guarantees of state-backed currency while stablecoins are issued by non-government entities [4].

One of the key differences between CBDCs and traditional digital forms of money, like bank deposits, is that a CBDC provides significantly more design flexibility. This flexibility includes a broad array of choices about who is given access to the currency, how the currency is distributed, the mechanics of payments, and the scope and nature of digital identity. Most of these design choices are not binary but instead

The design of money has reflected regulatory objectives since at least the 1660s, when the English Treasury issued silver coins with ridged edges to dissuade the illegal chipping of coins [1]. As central banks around the world explore the roll out of CBDCs [2], they are presented with an unprecedented opportunity to operationalize policy objectives through the design of these new digital currencies. One such objective is to ensure that any new currency does not play into the hands of criminals seeking to launder illicit funds or finance terrorist activities. This article explores how CBDCs provide new avenues to operationalize policy objectives related to anti-money laundering and countering the financing of terrorism (AML/CFT) through the design of the CBDC itself. It may come as a surprise that digital currencies, often associated with pseudonymity and obfuscation, can be designed to be inherently resistant to money laundering. However, we will illustrate that some of the features of digital currencies that are used to conceal details about transactions can also be used to create a currency more resistant to money laundering. More generally, we hope to provide a high-level perspective on how to think about designing CBDCs to meet regulatory objectives related to AML while balancing other priorities. After a brief primer on CBDCs, we will present the key dimensions of international AML regulation before discussing potential ways that a CBDC could be designed to operationalize these regulatory features. AML priorities do not exist in a vacuum, and so we will subsequently discuss how privacy, financial inclusion and compliance costs can be in tension with AML and how thoughtful CBDC designs can compromise between these competing objectives. Finally, we will explore how CBDCs provide opportunities to measure the effectiveness of different design choices to permit dynamic and evidence-based design approaches.
exist on a spectrum. For example, a distinction is often made between CBDCs distributed to the public directly, i.e., “single-tier”, and CBDCs distributed by commercial banks, i.e., “two-tier”. However, there are hybrid models that fall between the single- or two-tier distinction, such as the Bank of England’s proposed CBDC design where the central bank provides the core payment functionality, but authorized interface providers serve as intermediaries between the central bank and individual users. These interface providers can build additional services on top of the central bank’s basic functions; however, the central bank maintains the whole transaction ledger [5].

CBDC design choices are not merely technical in nature; they can also be used to operationalize policy objectives in sophisticated ways. As a result, policy objectives can and should guide the design of a CBDC. While this article focuses on AML, there are other important priorities – ranging from financial inclusion to national competitiveness – that may be advanced with thoughtful CBDC design. After explaining some key requirements of international AML regulation and how a CBDC could operationalize these, we will turn our attention to other policy objectives that exist in tension with AML and explore how thoughtful design choices can help to resolve these tensions.

Defining money laundering: When a criminal enterprise spends its ill-gotten gains, it risks attracting the attention of law enforcement. Money laundering is the process criminal organizations use to legitimate their profits so they can be spent without attracting attention [6]. Financing terrorism encompasses a wider array of activities that seek to provide funds to further terrorism (1). The two activities, money laundering and financing of terrorism, are often lumped together as both aim to obscure the true source or destination of funds. As a result, many of the interventions aimed at curbing money laundering also undermine the financing of terrorism and vice versa. We, too, will focus on approaches that address both issues.

Current AML Regulation: Countries around the world have formulated rules to combat money laundering, and most of these regulations focus on the same key areas. International standards around AML/CFT are set by the Financial Action Task Force (FATF), an inter-governmental organization which publishes a set of recommendations on AML/CFT [7]. In addition to the general recommendations, FATF also issued an updated guidance that highlights how its recommendations should be applied to virtual assets, including CBDCs, and virtual asset service providers [8]. The United States has two main sources of law relating to AML and CFT, namely the Bank Secrecy Act (BSA) and the USA PATRIOT Act (2,3).

Customer due diligence (CDD): FATF Recommendation 10 requires that financial institutions conduct CDD when they establish a new business relationship or when they carry out large or suspicious transactions. CDD goes beyond just identifying a customer by name or social security number; it also requires a financial institution to understand the nature of the business relationship with the customer. Financial institutions are expected to use this insight to determine whether a given transaction is consistent with the customer’s business profile.

In its updated guidance, FATF clarifies that when the risks of money laundering or terrorist financing are high, a financial institution should perform enhanced CDD [8]. FATF states that virtual assets may inherently pose a heightened risk and therefore require enhanced CDD which may involve tracking a customer’s IP address or conducting blockchain analytics. Financial institutions should consider risk factors related to the customer, geography, and the nature of services in determining whether enhanced CDD is appropriate. Enhanced due diligence also requires a financial institution to “increase the degree and nature” of its standard monitoring, which may include obtaining more information about the customer or transaction or examining the customer’s transactions more frequently.

In the U.S., under the USA PATRIOT Act, financial institutions are required to collect sufficient information about customers to enable them “to form a reasonable belief [about] the true identity of each customer” (2). The due diligence process requires a bank to record personal information such as a social security number and government issued IDs to verify that the person opening an account is who she says she is (4). FinCEN has begun to ramp up its enforcement in the cryptocurrency context and issued a guidance that underscores the obligations for cryptocurrency exchanges and similar businesses to also implement due diligence programs (5).

Suspicious Transaction Reporting (STR): FATF Recommendations 20 requires that financial institutions report transactions suspected of relating to criminal activities to the relevant law enforcement body. In the context of virtual assets, FATF suggests that countries should update their STR process to ensure that any tip-offs are valuable to law enforcement efforts by including information like “device identifiers, IP addresses with associated time stamps, virtual asset wallet addresses, and transaction hashes.” FATF has
also published a set of “Red Flag Indicators” that aim to help virtual asset service providers identify suspicious transactions [9]. These indicators relate to the size and frequency of transactions, transaction patterns, customer anonymity, sender or recipient behavior, sources of funds, and geographic risk factors.

Under the BSA, an institution must file a Currency Transaction Report whenever a transaction in excess of $10,000 is made [10]. A financial institution must also make a Suspicious Activities Report if it knows or has reason to believe that a transaction over $5,000 is related to illegal activities or does not fit a particular customer’s usual behavior (6).

Record Keeping: FATF Recommendation 11 requires financial institutions to maintain records about transactions and information collected during CDD. This data should be sufficient to enable law enforcement to reconstruct a customer’s transactions. The Updated Guidance clarifies that virtual asset service providers may not rely only on information contained on public ledgers for record keeping, as they must also record the customer’s identity and the nature of transactions. Under the BSA, a financial institution is required to retain records that document its regulatory compliance including data on customer accounts and transactions as well as information collected as part of CDD and transaction reporting [11].

The rules and standards described above aim to deter and detect criminal activity; however, they can lead to unintended consequences. The following section will briefly explore the conflict between AML and other important policy objectives.

Tension between AML and other objectives: AML priorities do not exist in a vacuum, and they may at times be at odds with other objectives. The success of a CBDC hinges on its adoption, and it would be counterproductive to design a CBDC that is resistant to money laundering but fails to attract widespread use. CBDCs provide promising new opportunities to better balance AML with other goals. This section will describe the tension between AML and privacy, financial inclusion, and compliance costs.

Privacy and AML: The priorities of AML and privacy are naturally at odds as detecting and investigating money laundering requires personal data about transaction parties and the behavior of individuals. In fact, individuals may be asked for highly sensitive and personal information as part of the CDD process, including, in extreme cases, information about an individual’s sexual partners [12]. Currently, there exists little privacy for consumers vis-à-vis financial institutions and regulators. For example, the EU only requires that data collected for AML not be used for business purposes but it does not impose privacy safeguards, like data minimization, on financial institutions (7).

Financial Inclusion and AML: An inclusive financial system gives all individuals and businesses “access to useful and affordable financial products and services that meet their needs” [13]. The pursuit of AML objectives can undermine financial inclusion in several ways. First, barriers to accessing the financial system that aim to deter criminals can also make access to financial products cumbersome or costly for legitimate users. Second, incentives for financial institutions to avoid doing business with criminal entities can prompt them to avoid doing business with individuals perceived to be high risk, regardless of their actual criminal intent. This practice, known as “de-risking”, undermines financial inclusion and tends to disproportionately impose costs on low-income communities such as those relying on remittance payments [14]. De-risking may also undermine AML efforts by forcing individuals to find alternative financial partners that lack sufficient AML capacity [15].

Compliance Cost and AML: The current AML regulatory regime imposes significant costs on both the public and private sectors. It is estimated that the global private sector spends over $200 billion annually on financial crime compliance [16]. Meanwhile, FinCEN alone requested a budget of $200 million for 2022, which represented a 50% increase compared to the prior year [17]. Part of these costs stem from the fact that the AML compliance regime emphasizes processes rather than outcomes [18]. As a result, financial institutions are disincentivized from finding efficient solutions and instead encouraged to spend more on AML compliance to avoid sanctions [19]. This, in turn, increases the public sector’s cost of processing reports from financial institutions.

Having explored the key dimensions of AML regulation and the tensions between AML and other goals, we will now focus on CBDC design choices that support AML objectives in a balanced manner.

Designing CBDCs to prevent money laundering and the financing of terrorism

Although it is extremely challenging to prevent criminals from using a currency system, a system designed to facilitate the detection of criminal behavior is less attractive for criminal use. This section builds on our discussion of AML regulation to explore CBDC
Digital identity and customer due diligence: For AML purposes, users in a CBDC ecosystems need to be identifiable and this digital identity can be designed to largely automate and facilitate the CDD process. In pseudonymous cryptocurrencies, identity is simply an address that is associated with a balance. Individual users are responsible for maintaining control of this identity [20]. In traditional financial settings, identity is more complex. Financial institutions collect information about a host of attributes including legal names, identification documents and information about an individual’s source of income. Upon opening an account, an individual receives an account number that is tied to a balance and which can be used to engage in transactions. The financial institution maintains the connection between the individual’s personal attributes and her account.

The traditional approach to identity relies on trust and introduces redundancy into the CDD process. In the traditional system, both customers and transaction counter-parties must trust financial institutions. Customers must trust financial institutions to handle their data responsibly while counter-parties must trust that due diligence is thorough. Redundancy arises when a customer seeks to do business with several financial institutions as each must conduct independent CDD. From an AML perspective, the traditional approach has benefits and drawbacks. The primary benefit is that individuals with criminal intentions face a challenge when accessing the financial system. Moreover, the redundancy inherent to the CDD process means that an incorrect entry is unlikely to be relied on by multiple financial institutions. Relatedly, each financial institution is incentivized to conduct thorough CDD to avoid sanctions. The drawback is that redundancy results in a process that is not standardized and the quality of due diligence may vary significantly between institutions.

A CBDC could provide an opportunity to leverage digital identity in ways that better address the risk of data breaches, the need for trust in financial institutions and the degree of redundancy. It is likely that a person’s identity in a CBDC network would be connected to an existing and more universal form of identity. For example, the ID2020 Alliance proposed a flexible technical framework for an interoperable and portable form of digital identity which can be implemented in various different contexts [21]. A CBDC could build on this type of identity by connecting information related to CDD to an individual’s digital identity. Individuals could submit their data to a trusted third-party that performs CDD and issues a portable CDD credential that can be used to open a CBDC account with any financial institution. Depending on the type of documents that are submitted, the individual may be prompted to update the information occasionally, but she would not need to start the process from the beginning. This model of “decentralized trust providers” is already in use: firms like Akoya act as intermediaries to give individuals more agency over their financial data while general purpose approaches like Open Algorithms (OPAL) allow data intermediaries to share insights without revealing raw data [22].

A solution involving a trusted intermediary offers benefits over the status quo in terms of AML effectiveness and other related considerations. First, it promotes more frequent updating of customer information and standardization across financial institutions, and therefore makes it is easier to utilize the collected data or to institute improvements to the CDD process. Second, the approach reduces redundancy, and thus cost, because an individual can open multiple accounts but only undergo CDD once. Third, from a privacy perspective, the approach obviates the need for an individual to submit data to multiple financial institutions directly, reducing the risk that the data is misused. Fourth, the outlined solution reduces the need for trust in third parties. While an individual must still trust the intermediary performing CDD, these intermediaries are likely to have reduced conflicts of interest compared to financial institutions as they exist exclusively to perform CDD and so are less prone to use data obtained as part of due diligence for other purposes. Reducing these conflicts of interest further helps to address de-risking by making the CDD process independent of other incentives. As we will discuss shortly, by gathering data on financial inclusion, the CDD process could be refined iteratively to ensure that categories of individuals, such as immigrants sending remittance payments, are not systematically denied access to the CBDC.

If a CBDC is intended to replace not just bank deposits but also cash, this raises additional considerations. Today, cash provides an anonymous form of money for relatively small transactions. Users of cash do not necessarily need to undergo CDD.
although most cash users will draw cash from a bank account and large cash transactions may be reported as suspicious. A CBDC could be designed to completely eliminate anonymous cash transactions. However, it is also possible to design a system that allows for small transactions to largely proceed anonymously with the ability to determine the payee’s identity under exceptional circumstances. The cryptographic foundation for this approach was laid by Chaum’s Algorithm in 1983 and it has since been implemented by cryptocurrencies like DigiCash and GNUTaler [23]–[25]. There is a risk that a CBDC could win the battle but lose the war against criminal misuse by failing to be attractive to a wide enough user base. Allowing small CBDC transactions to proceed anonymously may be critical to attracting users.

Suspicious transaction reporting (STR) and collaborative transaction monitoring: Financial institutions today are expected to report transactions that they deem suspicious. The bar for what needs to be reported is relatively low: for example, in the United States, a report must be made for suspicious transactions over $5,000. Financial institutions have an incentive to over-report suspicious transactions to avoid facing sanctions as the cost of investigating these reports is carried by government agencies. If the practice of “crying wolf” is widespread, then genuine illegal transactions may be missed in a sea of reports. In a CBDC, the STR process could be redesigned to better address money laundering risks by facilitating collaborative monitoring and leveraging algorithmic approaches.

Individuals and businesses do not engage in financial transactions at random; for most of us there is a network of relationships that gives rise to frequent transactions while there are some people with whom we only transact on occasion. Moreover, the probability that we engage in a financial transaction with someone is a function of our closeness in the transaction network. For example, we are more likely to visit a new coffee shop frequented by a friend than a coffee shop that no one in our network has been to. While today’s financial institutions can only see a fraction of the transactions that take place, a CBDC can facilitate collaboration between financial institutions to identify nefarious actors. This collaboration does not necessarily require centralizing transaction data or sharing personal data, instead pseudonomized data together with insights about how people tend to interact can help spot suspicious transactions (see Figure 1). Smart contracts – self-executing programs in cryptocurrency networks that automatically trigger actions when a set of conditions is satisfied – could operationalize this type of collaboration. Different financial institutions could share pseudonomized transaction data with a smart contract that analyzes the data and issues a report when a pattern of transactions fulfills certain predefined conditions, for example repeated transactions involving parties far outside of one’s network. Law enforcement agencies would determine what these criteria should be.

In today’s financial ecosystem, individual institutions have an incentive to over-report, but they do not bear the cost of this reporting. By contrast, in a CBDC, reporting can be based on a data-driven quantification of risk related to different transaction patterns. STR in a CBDC system can be iteratively modified to maximize detection and minimize over-reporting. The outlined approach to STR would reduce both redundant infrastructure across financial institutions and the number of reports made to government agencies, thus reducing total AML costs. In combination with a well-designed digital identity solution, the proposed approach could also address privacy concerns, as financial institutions would no longer need to send personal data to government agencies. Instead, government agencies would receive pseudonymous account numbers associated with suspicious transactions. If the agencies choose to investigate, they could connect these account numbers back to an individual user’s data that is administered by a trusted intermediary. Moreover, de-anonymization
for law enforcement purposes could require additional authorization, similar to a search warrant. This solution could thus minimize the amount of personal data that is needlessly shared while allowing law enforcement operations to proceed.

Record Keeping in a CBDC: Both the FATF Recommendations and U.S. laws emphasize the need for financial institutions to maintain records about their customers and their transactions. There are two broad categories of data that need to be recorded. The first is data about transaction parties that is normally collected as part of the CDD process. The second is data about a particular transaction. Today, financial institutions record both categories of data, but in a CBDC these two categories could treated separately.

Record keeping of transaction data would be a necessary part of any CBDC to permit ex-post auditing. To balance the need for rigorous record keeping with privacy concerns, CBDC record keeping infrastructure for transaction data should focus on several key properties:

- Independence from the medium of transfer: A given CBDC data network should operate independently from other CBDC networks and other virtual currency networks. Record keeping entities should be separate from currency flows [26].
- Interoperability with CBDC and virtual asset networks: A CBDC would likely coexist with many other currency networks, and interoperability between these networks undermines money laundering by facilitating collaborative detection. Therefore, a CBDC data network should provide standard interfaces that permit all virtual asset networks to integrate their record-keeping functions based on standard data formats.
- Owned and operated by a public-private collaboration: The CBDC data network should be a private-public collaborative effort that seeks to provide stability to the “main street” economy as it transitions into the age of digital currencies.
- Employs data privacy protection technologies: The CBDC data network should provide ongoing upgrades to its privacy-protection technologies, utilizing new forms of privacy protection for data-in-transit, i.e., between endpoints within the network, and data-in-storage.

A CBDC system must also maintain records of personal data, including data that is collected as part of the CDD process. In the traditional financial system, individuals have minimal agency over their data: once data is submitted as part of CDD it is very difficult to limit or monitor who has access to it. Of course, legitimate law enforcement requires access to personal data, and it may not always be possible or even desirable to alert individuals to the fact that they are under investigation. However, well designed data governance solutions and new advances in data analytics can be leveraged to better balance individual agency over data and law enforcement requirements. In the context of CDD, we already discussed how a trusted intermediary could perform due diligence. This intermediary could also be tasked with record keeping. In terms of data governance, the intermediary could be structured as a third-party data trust that owes fiduciary duties to the individuals whose data it administers [27]. Law enforcement agencies could obtain data from these data trusts, but this may require special authorization similar to a search warrant. Using a data trust model to conduct record keeping would also introduce the concept of data minimization to AML. Unlike today’s financial institutions, which have limited incentives to minimize the amount of data shared with financial regulators, the third-party data trust model explicitly prioritizes data protection. These data trusts would also be able to reveal aggregated insights about financial data which may be important to the continued improvement of CBDC designs. To this end, the trust could take advantage of new approaches to data analytics that allows insights to be drawn from encrypted data [28]. Encrypted data could be used to obtain system-level insights about how a CBDC is functioning without requiring raw data. It is also possible that suspicious behavior could be identified in encrypted data to permit subsequent investigation by law enforcement. Overall, well designed data governance solutions can be used in concert with sophisticated data analytics approaches to store and use personal data securely and maximize individual agency over this data while facilitating the investigation of money laundering.

CBDC networks and transfer gateways: In designing for new CBDC infrastructures, it is especially important that the identities of key service providers in the network are known and validated. In particular, CBDC service providers that conduct cross-jurisdiction currency transfers could employ gateways specifically designed for such transfers. These gateways represent policy-enforcement points where network-level policies as well as community-level policies are enforced for incoming and outgoing transfers. Engineering efforts to define interoperable gateways for asset transfers are underway at the Internet Engineering Task Force (IETF), the voluntary open-source standards organization which
defines technical protocols for the internet [29].

**Iterative legal design**

The prior sections presented some examples of opportunities to take advantage of CBDC designs to operationalize AML objectives while balancing competing priorities. However, a key insight of computational legal approaches is that regulatory design should not be thought of as a one-time exercise but rather an iterative process that seeks to continuously improve regulation based on its real-world performance [30]. In addition to the definition of regulatory objectives and policies seeking to achieve these objectives, successful iterative legal design requires metrics to assess the efficacy of legal systems and opportunities for redesign. As we outlined, the nature of CBDCs allows us to embed regulatory objectives into the design of the digital currency. This section will highlight some opportunities to measure the effectiveness of these designs to permit evidence-based redesign.

CBDCs provide ample opportunities to collect data on how well regulatory objectives are addressed. In our view it will be critical to the success of any CBDC to continuously gather and analyze data on the performance of its design and to update the design in response to these insights. A basic measure of AML efficacy is the number and type of money laundering incidents that are identified by law enforcement agencies. Other metrics might involve comparing the CBDC to other payment systems or tests that seek to determine whether certain patterns of behavior result in appropriate reporting. Financial inclusion could be measured through aggregated statistics on the composition of the CBDC community based on data collected as part of the CDD process. For that purpose, it will be important to determine approaches to data aggregation that ensure the privacy of CBDC users is respected. A benefit of the proposed record keeping system is that data trusts, which would owe legal duties to the individuals whose data they administer, would perform the necessary aggregation and ensure that no personal data is leaked in the process. Privacy is somewhat more challenging to measure as it relates not only to objective metrics, such as the number and severity of data breaches, but also to a subjective assessment of whether users feel that their privacy is respected. Privacy might also be proxied by the usage of cryptocurrencies that provide a heightened degree of anonymity. In addition, user surveys and interviews might be used to determine whether individuals feel that the CBDC provides sufficient privacy protection.

Defining reliable metrics for the performance of CBDC designs is only half the battle, as these insights need to be used to subsequently adjust the CBDC design. In some cases, it may be desirable to test new designs on a subset of users and to measure the results before rolling out changes to the entire system. In any case, a CBDC should provide regular opportunities for re-design to optimally address policy objectives and to cater to changing needs. Not only the CBDC design but also the metrics used to assess it should be regularly scrutinized, especially in response to serious system failures. Such investigations could be modeled after the thorough investigations of airline accidents that seek to precisely identify what system failures were responsible for an accident and what changes would prevent similar future accidents. As an example, see the extensive report on the Concorde accident [31]. Ultimately, by actively measuring the performance of a CBDC system and making continuous improvements, its design can be optimized to work towards solutions that address policy objectives and trade-offs between competing objectives.

It is unlikely that even an iterative process can result in a monetary system that is completely resistant to criminal behavior, and even an extremely well designed CBDC would likely provide some opportunities for illicit transactions to slip through its cracks. More importantly, a monetary system as a whole is only as effective against money laundering as its weakest link. In a world where CBDCs coexist with other forms of payments, including cash and cryptocurrencies, criminal organizations will seek alternative ways of concealing their transactions. Nonetheless, it is critical to the success of CBDCs to have national and international buy-in. An inherent resistance to money laundering can help achieve this. If a CBDC is designed to address a broad enough array of financial needs better than other alternatives, then individuals will gravitate towards using it. In such a future, the use of other forms of payment may even give rise to reasonable suspicion as it signals a desire to avoid scrutiny. While such a future is clearly still far away, the concepts sketched out here highlight the synergies between an accessible and convenient CBDC design and long-term AML goals.

**Conclusion**

The introduction of CBDCs provides an unprecedented opportunity to rethink how we achieve AML/CFT objectives. By emphasizing regulatory goals early in the CBDC development process, we can operationalize these objectives through the design of the CBDC itself. Not only can CBDCs automatically further policy objectives, but a digital currency may also facilitate data collection which can be used to continuously measure and improve the performance of its design. It is our hope that as the international community continues to explore CBDCs, policy objectives will guide the design
process. However, there are risks associated with focusing too narrowly on any single regulatory dimension. It seems to be in every nation’s interest to retain control over the money supply and to compete with private forms of money effectively. Therefore, the tension between competing objectives must be an acknowledged part of the design discussion to help identify technical approaches that provide sustainable middle-ground solutions.

Acknowledgements
We would like to thank Shlomit Wagman, John D’Agostino, Denis Avrilinos, Sangita Gazi, and two anonymous reviewers for their thoughtful feedback.

Citation

Open Access

This *MIT Science Policy Review* article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third party material in this article are included in the article’s Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article’s Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit http://creativecommons.org/licenses/by/4.0/.

Legislation Cited

(1) 18 U.S.C § 2339C - Prohibitions against the financing of terrorism.
(2) Bank Secrecy Act of 1970, 31 USC 5311 et seq.
(4) 31 CFR § 1020.220 - Customer identification program requirements for banks.
(6) 31 CFR § 1010.311 - Filing obligations for reports of transactions in currency.

References


[31] Cramoisii, G. Air crash investigations: The end of the Concorde era, the crash of Air France flight 4590 (2010).