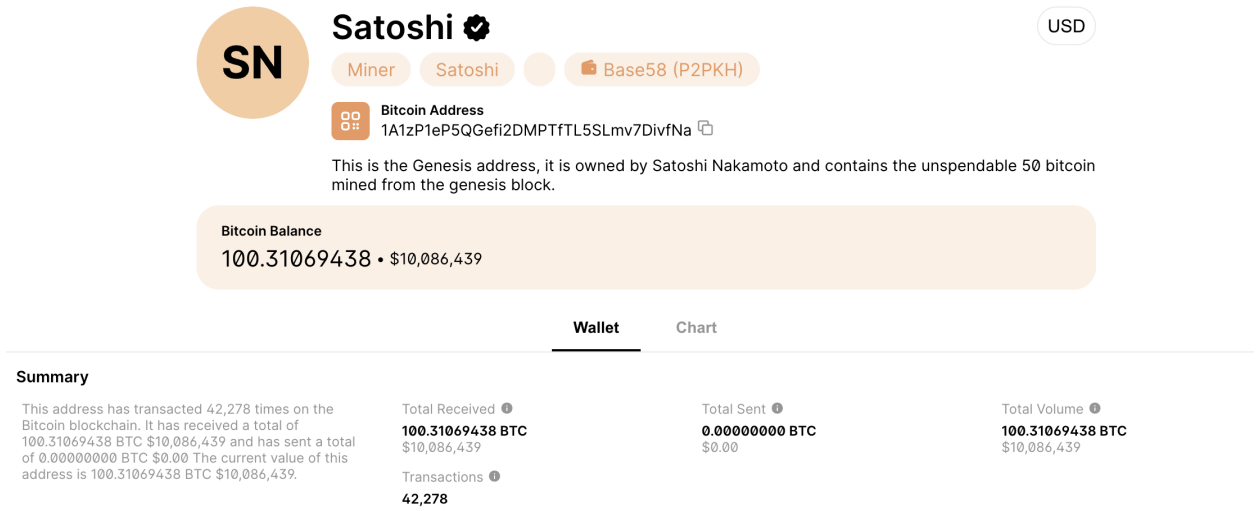
BPUK Commentary on CARF reporting framework

by Webmaster | January 16, 2025 | Bitcoin Policy, Featured, News, Research



The Cryptoasset Service Providers (Due Diligence and Reporting Requirements) Regulations 2025 (technical guidance and response to consultation request).

We refer to the draft regulations: The Cryptoasset Service Providers (Due Diligence and Reporting Requirements) Regulations 2025 (the "**Regulations**"). Capitalised terms used but not otherwise defined in this paper shall have the meanings given to them in the Regulations.

We note that in November 2023, the former government declared that it intended to adopt the Organisation for Economic Co-operation and Development's Cryptoasset Reporting Framework ("**CARF**"). During the spring of 2024, a consultation began to gather opinions on how to enact these new regulations along with other suggested changes. The government has now released preliminary drafts of the CARF Regulations, which are accompanied by a summary of the feedback received during the consultation. Our commentary and recommendations are below.

Executive Summary

RECOMMENDATION to clarify the extent and limitation of applicability of the Regulations

HMG has an opportunity to improve upon some of the deficiencies of CARF by making clear the extent of the applicability of the CARF rules. Relevant examples in the United States, from FinCen guidance and the US Fifth Circuit Court's ruling relating to Tornado Cash are supportive of the view that (i) the code that constitutes Bitcoin Core is not an 'entity' for the purposes of the Regulations and (ii) the developers of self-hosted wallet software are therefore not caught by and should not be subject to the obligations imposed by the Regulations. The Regulations would benefit from such clarity.

While these conclusions are implicit from a close reading of the Regulations as drafted, the secondary legislation would be greatly improved by the inclusion of clarificatory language to this effect, and to make it clear that open source developers of relevant software shall be excluded from scope and shall not face any reporting obligations pursuant to the Regulations.

RECOMMENDATION to limit the amount and nature of personal information gathering so as to reduce the risk of personal harm to crypto-asset holders.

We strongly recommend that the extent of the information-gathering requirements included in CARF are revisited by HMG when preparing the final draft of the Regulations. Proportionate limitations could include:

(i) limiting disclosures only to those where a user has in one financial year made disposals of crypto-assets that might exceed a material threshold (such as the £200k limit generally relevant for monitoring purposes in an income tax context), and then only retaining that information for a limited period (such as three tax years or less);
(ii) ensuring that *de minimis* levels are included and set appropriately, thus reducing both the burden of compliance for a relevant CASP and the risk of wholesale disclosure of a person's crypto-asset holdings following data breaches; and
(iii) not sharing real names and addresses other than in limited circumstances, and never in plain text, unless a user can be shown to have made disposals in excess of the tax-free personal allowance.

These recommendations are made owing to the extreme risk of (i) data breaches and (ii) consequential extreme physical harm to crypto-asset users. Evidence of each is included in the body of our submission.

We also note that the government is seeking technical feedback on the draft Regulations to ensure they operate as the government intends and to identify any areas which need further clarification in more detailed guidance. In response to this request, we have drafted and wish to submit the feedback below, focusing on two key areas in relation to the Regulations, namely:

1. **Scope and exclusions**; and
2. **Privacy and personal safety concerns**, which are of particular relevance to Bitcoin and other cryptocurrencies in a manner unique to these assets, and one that may not be apparent to those unfamiliar with the way in which cryptoassets are typically held and used.

(1) Scope and exclusions

The Regulations track the CARF definitions in determining to whom it is applicable. Key to this determination is whether or not a person (natural or otherwise) is a 'reporting cryptoasset service provider' ("**RCASP**" or "**CASP**"). Broadly, for the purposes of CARF, a "Crypto-Asset Service" is defined through the scope of activities performed by such a person.

A crypto-asset service includes any service provided by an individual or entity that, as a business, effectuates exchange transactions for or on behalf of customers. This could involve acting as a counterparty to exchange transactions, serving as an intermediary to exchange transactions, or making available a trading platform for crypto-assets.

Relevant services might cover transactions such as exchanges between crypto-assets and fiat currencies, between one or more types of crypto-assets, or transfers of crypto-assets, including for payment of goods or services, and transfers to what are typically referred to by regulators as 'unhosted wallets' but which should more correctly simply be called 'wallets' as they are fundamental to the architecture of how such systems work. It is essential for regulators and lawmakers to remember and understand that the functioning of the Bitcoin system would not be affected were every CASP to go out of business tomorrow; for the system is at its simplest one of peer to peer electronic cash and does not require any CASP to be functioning or even in existence in order for it to continue operating. Bitcoin transactions would continue to be made peer to peer and processed regardless.

CARF specifically aims to ensure the collection and automatic exchange of information on crypto-asset transactions to enhance tax transparency and compliance. Entities involved in these activities are required to perform due diligence on their customers, collect information about them, and report on transactions to tax authorities, who may then exchange this information internationally with the intention of combatting tax evasion.

The definition of CASP encompasses a broad range of service providers in the crypto-asset space, including but not limited to cryptocurrency exchanges, brokers, dealers, and ATM operators, but generally excludes providers of services that are purely decentralized where no entity has sufficient control to comply with reporting obligations. It is upon this exclusion that we wish to focus, particularly given the implications of recent case law emerging from the United States.

The obligations in the Regulation pursuant to Part 2 apply to 'UK reporting cryptoasset service providers' and cross-refer to CARF in order to determine whether the CARF provisions apply to a person. A person will be a CASP for the purposes of the regulation if they are:

1. an entity or individual resident for tax purposes in the UK;
2. an entity that (a) is incorporated or organised under the laws of England and Wales and (b) either has legal personality in England and Wales or has an obligation to file tax returns or tax information returns to the tax authorities in the UK with respect to the income of the entity;
3. an entity managed from the UK; or
4. an entity or individual that has a regular place of business in the UK.

We note that the above CARF definition uses the term 'entity' throughout; this is itself defined as "a legal person or a legal arrangement, such as a corporation, partnership, trust, or foundation."

While CARF does include a definition of "Excluded Person", this term is used in the context of certain Entities that are not subject to reporting under CARF because (it is alleged) they represent limited tax compliance risks. Where we believe CARF is deficient – and where we believe the Regulations can improve upon CARF – is in further consideration and delineation of where and to whom the Regulations cannot and should not apply.

Above, we noted the significance of a recent legal ruling in the United States, which, while not applicable in England and Wales, nevertheless may have a significant impact on the interpretation and application of rules and regulations relevant to crypto-asset transactions. In November 2024, a three-judge panel of the United States Court of Appeals for the Fifth Circuit reversed a Texas District Court's decision and overturned the US Department of the Treasury's Office of Foreign Assets Control ("**OFAC**") sanctions designations against certain smart contracts associated with decentralized virtual currency "mixer" Tornado Cash. The decision related specifically to the question of whether the computer code constituting the Tornado Cash smart contracts could be "property" for the purposes of OFAC.

The Fifth Circuit held that "Tornado Cash's immutable smart contracts (the lines of privacy-enabling software code) are not the "property" of a foreign national or entity, meaning (1) they cannot be blocked under IEEPA (the International Emergency Economic Powers Act), and (2) OFAC overstepped its congressionally defined authority." However, the court did not consider under the relevant statutes whether Tornado Cash qualifies as an 'entity' capable of being sanctioned, even though it held that the immutable Tornado Cash smart contracts are not capable of being owned because they operate without "the option for anyone to update, remove, or otherwise control [the] lines of code." In fact, the court noted that even in the wake of OFAC's sanctions, the Tornado Cash smart contracts continue to operate unimpeded for "anyone with an internet connection." The decision is nevertheless supportive of the view that an immutable smart contract cannot be considered sanctionable property, and further decisions may also support the view that the developers who work on such software cannot be considered 'CASPs' for the purposes either of CARF or the Regulation.

Secondly, we cite the approach taken by the European Union towards the developers of hardware and software products that enable users to take self custody of their assets. The key regulation in this context is Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (the "**AML Regulation**").

To prevent the illicit use of crypto-assets, the AML Regulation prohibits the provision and custody of anonymous crypto-asset accounts or accounts allowing for the anonymisation or increased obfuscation of transactions by crypto-asset service providers, including through anonymity-enhancing coins. Such prohibition does not apply to providers of hardware and software or providers of self-hosted wallets insofar as they do not possess access to or control over those crypto-asset wallets (Recital 160 and Article 79 AML Regulation). We quote from Recital 160, which provides helpful clarification: "*In order to ensure effective application of AML/CFT requirements to crypto-assets, it is necessary to prohibit the provision and the custody of anonymous crypto-asset accounts or accounts allowing for the anonymisation or the increased obfuscation of transactions by crypto-asset service providers, including through anonymity-enhancing coins.* ***That prohibition does not apply to providers of hardware and software or providers of self-hosted wallets insofar as they do not possess access to or control over those crypto-asset wallets.***" [our bold italics]

This approach, while addressing the legitimate aim of preventing illicit use, acknowledges the economic and factual reality that the developers of relevant software and hardware products do not have any control over the assets held by the users of their products, and correctly exempts such developers from obligations in this context.

We would draw a comparison between the developers of free and open source software ("**FOSS**") of all kinds and those developers working on such FOSS that is used by Bitcoin users across the world, whether in the form of wallet software or the fundamental piece of Bitcoin software, Bitcoin Core itself. Bitcoin Core is the primary software implementation of the Bitcoin protocol. It is the software that runs the nodes making up the Bitcoin network, validating transactions and blocks according to Bitcoin's consensus rules, and includes wallet functionality allowing users to transact freely and on a peer to peer basis, entirely without the assistance of a CASP. Furthermore, Bitcoin Core entirely fails to meet the four requirements for a CASP as set out in CARF and as applicable to the Regulation; it fails these *ab initio* in that, like the Tornado Cash smart contracts, it is simply a piece of software and is not an entity at all, let alone having the benefit of a controlling mind or a jurisdiction of incorporation.

As we note above, while the conclusion is implicit, CARF has failed to make it sufficiently clear that open source software such as Bitcoin Core cannot be considered an 'Entity' for the purposes of CARF, and furthermore that software developers who contribute to the code of Bitcoin Core or to other wallets also cannot be considered 'Entities' within the scope of the rules. The Regulations

would benefit from constructive clarificatory language as included in the AML Regulations quoted above.

Guidance published in 2019 by the United States Financial Crimes Enforcement Network ("**FinCen**") supports this view, inasmuch as software developers or wallet providers are not – and should not be – considered or regulated as money service businesses. Section 4.2.1 states that software wallet providers (i.e., "non-custodial" or "unhosted" wallet providers) are not regulated as money transmitters. And section 4.2.2 states that multi-sig providers without the ability to (unilaterally) transact are also not regulated as money transmitters. The logic is simple: non-custodial wallet providers, because they do not have sufficient power to unilaterally execute or prevent transactions, are never able to accept or transmit currency or currency substitutes and therefore could not and should not be a "money transmitter" (a type of Money Service Business) under the US Bank Secrecy Act's implementing regulations, which require acceptance and transmittal. The same logic should apply to the implementation and applicability of the Regulations.

In summary, HMG has an opportunity to improve upon the deficiencies of CARF by making clear the applicability of the CARF rules, in a manner similar to the AML Regulation. Drawing from relevant examples in the United States, both the FinCen guidance quoted above and the Fifth Circuit's ruling relating to Tornado Cash are supportive of the view that (i) the code that constitutes Bitcoin Core is not an 'entity' for the purposes of the Regulations and (ii) the developers of self-hosted wallet software are not and should not be subject to the obligations imposed by the Regulations. Furthermore, the AML Regulation provides an up to date example of such clarificatory language that has been used in a relevant context in the EU regulation.

RECOMMENDATION: While these conclusions are implicit from a close reading of the Regulations as drafted, the secondary legislation would be greatly improved by the inclusion of clarificatory language to this effect, and to make it clear that open source developers of relevant software shall be excluded from scope and shall not face any reporting obligations pursuant to the Regulations.

(2) Privacy and personal safety concerns

This section deals with potential risks to the personal safety and well-being of Bitcoin and crypto-asset holders that are likely to result directly from the information collection, retention and disclosure requirements imposed by the Regulation and by CARF.

These risks emerge from the peculiar nature of the way in which the Bitcoin system functions, which may not be obvious or apparent to those responsible for drafting either CARF or the Regulation.

Information Gathering Requirements

The information gathering requirements to which we refer are set out in Section II A of CARF. Pursuant to the Regulations, a UK reporting cryptoasset service provider must comply with the reporting and due diligence requirements included in Section II A. These include (but are not limited to):

(i) names, addresses, jurisdiction of residence, and date and place of birth of cryptoasset users;

(ii) names and types of cryptoassets such users have purchased, including the aggregate amount paid;

(iii) aggregate gross amounts received, and amounts disposed of for fiat currency; and

(iv) aggregate fair market value of cryptoassets acquired, sold, transferred, or used in Reportable Retail Payment Transactions.

We note that the place of birth is not required to be reported unless the Reporting Crypto-Asset Service Provider is otherwise required to obtain and report it under domestic law.

Risks emerging in conjunction with implementation of the FATF Travel Rule

The Financial Action Task Force ("**FATF**") Travel Rule is a set of guidelines that require financial institutions and virtual asset service providers ("**VASPs**") to share data about transactions, subject to certain thresholds and carve outs. Under the FATF recommendations, VASPs are required to collect, verify, and transmit information about both the sender and the recipient of cryptocurrency transactions exceeding a certain threshold, typically $1,000. This includes transactions involving non-custodial or self-hosted wallets to ensure traceability and prevent money laundering or terrorist financing.

In the European Union, the Transfer of Funds Regulation ("**TFR**") applies the Travel Rule to crypto-asset transfers without a *de minimis* exemption, mandating disclosures for transactions from 'self-hosted' wallets to 'hosted' wallets and vice versa, and that in such circumstances the crypto-asset service provider must verify the ownership of the wallet. This involves collecting and possibly storing personal identity details of the wallet owner. The information collected is likely to include the details of the wallet address of the crypto-asset wallet holder on the relevant blockchain. It is at this point, in conjunction with the information-gathering requirements set out above, that the risks for crypto-asset users emerge, in addition to a potential and large-scale violation of their rights

to respect for their private and family life pursuant to Article 8 of the European Convention on Human Rights (the "**Convention**").

In short, the information pertaining to wallet addresses on chain, gathered pursuant to the FATF Travel Rule, in combination with the details that will be collected by CASPs including names, home addresses, and dates of birth, if subject to a hack or data leak could be easily cross-referenced by bad actors in order to determine where crypto-asset users live, and how much of a relevant asset they hold. This is almost certain to expose them, and their families, to an unacceptable risk of real and physical harm.

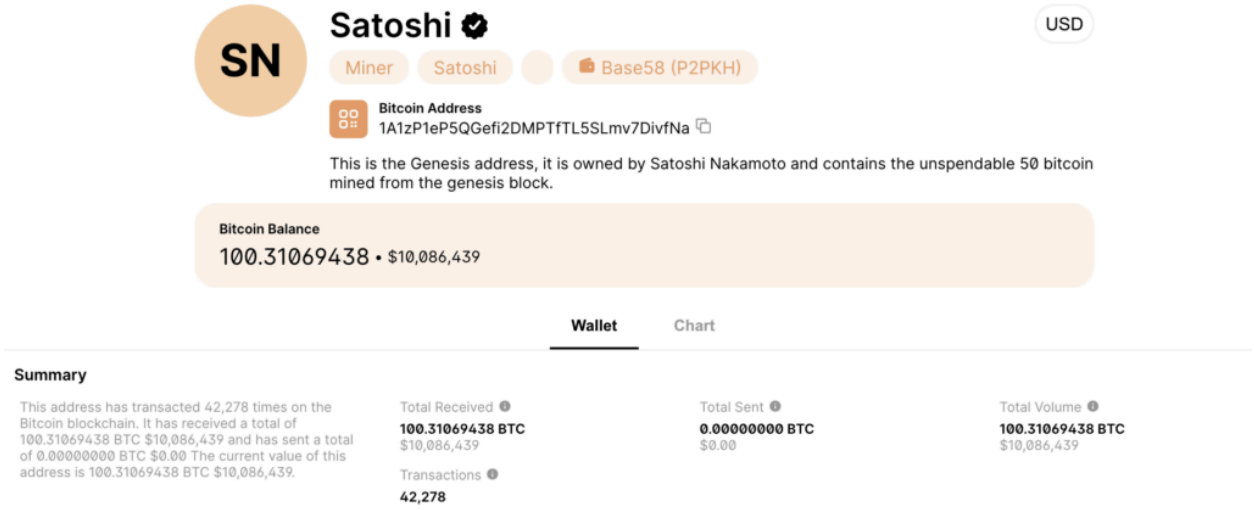
Neither CARF nor the Regulation would have been drafted in this way had their authors fully understood the absolute transparency and effective lack of privacy offered by crypto-assets. We will in this section use Bitcoin as an example, but the same principles hold true across the sector.

Bitcoin is frequently described in the non-specialist media as an 'anonymous cryptocurrency'. This categorisation is incorrect; Bitcoin is in fact pseudonymous, in that network participants transact using alphanumeric strings as identifiers, rather than names. These alphanumeric strings, commonly called 'addresses', 'wallet addresses' or simply 'wallets', provide infinitely more transparency than that afforded by the traditional banking system. Any person, anywhere in the world, with access to the internet, can easily look up a wallet address on a website known as a block explorer, and can see immediately how much Bitcoin is controlled by that address, and how often that address has transacted on the Bitcoin system.

Not only this, but each **transaction**, as well as each **address,** is also public, and transfers of Bitcoin may thus be traced from address to address with relative ease. It is this extreme level of transparency that ironically, and in contradiction to the myths promulgated by the non-specialist media, makes Bitcoin almost uniquely unsuited to criminal use of any kind. The records of transactions cannot be changed; they are permanent, accessible to all, and admissible in court as evidence. All that a law enforcement agency needs to do is to connect a wallet address to a person, and the evidence of their transactions is beyond challenge.

Unfortunately, all that a bad actor needs to do is to make exactly the same connection, and this is where the extreme risk of personal harm arises.

By way of example, I suggest a review of the address 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa being the address of the Genesis block and thought to be controlled by Satoshi Nakamoto. This can easily be viewed using a block explorer such as https://www.blockchain.com/explorer and shows the following:



As seen above, this wallet address contains a balance of 100 Bitcoin (of which 50 are spendable – the Genesis Coinbase transactions are unspendable). It is obvious that even a bounty of 50 Bitcoin would represent a considerable amount of money and if the name and home address of Satoshi Nakamoto were to be exposed, this would represent a significant risk to his, her or their personal safety.

This fact pattern arises because the financial asset (ie. Bitcoin) held by a Bitcoin user is not like money in a bank account. Not only is it possible for anyone, anywhere in the world, to see a person's entire transaction history, but it is also possible to hold extremely large amounts of value in one's own personal possession in a manner that is not typically replicated in the case of cash holdings. In the event of hostile action by a bad actor, a person may be forced through the threat of violence to transfer Bitcoin a hostile third party, and once transferred it is impossible to freeze such assets or prevent their free onward transfer by the bad actor, again by contrast with the traditional banking system, where bank accounts may be frozen and stolen funds more easily returned.

In summary, the collection of personal information pursuant to CARF, and the collection of wallet address information pursuant to the FATF Travel Rule, would appear in combination to pose uniquely acute risks to personal safety and personal property. These risks should be mitigated as much as possible, and the benefits do not appear proportionate to the risks involved, particularly considering how these impinge on a citizen's Article 8 Convention rights.

Nor is it sufficient to assert that any information gathered pursuant to the Regulations will be kept safe. Such information will be a valuable 'honey pot' for hackers and bad actors across the world. What follows is not an exhaustive list, but by way of example recent highly damaging breaches of sensitive personal information include:

(i) The theft of US Treasury documentation allegedly by Chinese state-sponsored actors in December 2024;

(ii) Details of UK armed forces personnel being exposed in a hack in early 2024;

(iii) Personal information of “nearly all” of the 109 million AT&T Wireless customers being illegally downloaded and copied in April 2024;

(iv) The personal information of all 6.5 million Israeli voters (including full names, addresses, and identity card numbers) being exposed in 2020;

(v) The theft of highly sensitive NHS patient data, including the results of blood tests for HIV and cancer, in June 2024, including details of 300 million interactions with the NHS; and

(vi) A cyber attack on Evolve Bank & Trust that exposed the personal data of at least 7.5 million customers early in 2024.

The non-exhaustive list above provides ample evidence that, at present, **no institution – whether the US Treasury Department, the UK Ministry of Defence, the NHS or a banking institution – appears capable of adequately protecting personal information and ensuring that such information is not stolen by or exposed to bad actors**. It is therefore safe to assume that if information is gathered at any point by such a body, it will sooner or later be accessed and exploited by bad actors. Consequently, we would strongly argue that the only way to ensure that such information is not exploited, and to prevent individuals from suffering harm as a result, **is not to gather the information in the first place**.

We contend that requiring the collection of and access to such financial data as required by CARF, the Regulation and the FATF Travel Rule may constitute an unacceptable interference with the customers’ right to financial privacy. The right to privacy is a fundamental human right aimed at protecting individuals from excessive interference by public authorities in their private lives. It encompasses private and family life, the confidentiality of correspondence, and the protection of financial data, including information as to non-custodial wallet addresses and transaction histories. This right is included in Article 12 of the Universal Declaration of Human Rights, Article 8 of the Convention, and Article 7 of the Charter of Fundamental Rights of the European Union.

Under Article 52 of the Charter of Fundamental Rights, any interference with the right to privacy is permissible only if it meets stringent criteria:

(1) it must be based on law;

(2) it must respect the essence of the right to privacy;

(3) it must be proportionate to the objective pursued; and

(4) it must be necessary and genuinely meet objectives of general interest or the need to protect the rights and freedoms of others.

Both the Regulations (as currently drafted) and the UK/EU implementation of the FATF Travel Rule pose significant risks to the right to privacy. The blanket approach, the lack of *de minimis* thresholds, and the absence of precise procedural safeguards increase the likelihood of violations and the misuse of data for purposes unrelated to crime prevention, such as political objectives,and the collection and retention of data is likely to increase the risks of physical harm being done to individuals following inevitable data leaks. While on the one hand these regulations entail substantial intrusions into privacy, they fail to ensure adequate protection of citizens' private lives and pay scant regard to their personal safety.

Examples of documented physical attacks on crypto-asset holders:

Jameson Lopp, the co-founder and CTO of Casa.io, has compiled an extensive list of known physical attacks against Bitcoin and crypto-asset holders. Some examples include:

Jameson Lopp Himself

Lopp was subjected to a SWATting incident where an anonymous caller falsely reported a hostage situation at his residence, leading to a significant police response. An inherent risk in a SWATting incident is that such a police response is typically an armed response and can result in physical harm to the resident. This was likely motivated by his public stance on Bitcoin philosophy and scaling debates.

Hal Finney – SWATting
Early Bitcoin pioneer Hal Finney and his wife experienced a SWATting event where police responded to a false report of a murder and potential suicide at their home. This incident was one of the first documented cases of physical attacks related to crypto assets.

Dwayne Richards – Kidnapping and Stabbing

Richards was kidnapped and stabbed in a horrific attack where the assailants knew that he held a significant amount of Bitcoin and targeted him as a result. This incident illustrates the extreme risk of violence and physical harm that cryptocurrency holders may face if their identities and the amount of their holdings become publicly known.

Pavel Lerner – Kidnapping and Ransom

Lerner, the owner of a Bitcoin exchange, was kidnapped and held for ransom, demonstrating how high-profile crypto-asset holders and users can become targets for physical threats. He was released only after payment of a million dollar ransom.

Remy St Felix – Multiple instances of violent home invasions and robberies

St Felix was a leader of a robbery crew that targeted cryptocurrency owners through violent home invasions. Between September 2022 and July 2023, St Felix helped to plan and orchestrate a series of robberies in Durham, North Carolina; Florida; Texas; and New York. Victims from St Felix's home invasions were kidnapped in their own homes and told to access and drain their cryptocurrency accounts.

Family member kidnapping, violent assault and death threats – New Year's Eve 2024

Two men targeted the France-based family of a crypto influencer who now lives in Dubai. The perpetrators allegedly invaded his father's home, tied up the family, and kidnapped the father. Next they contacted the influencer and demanded ransom, dousing the father with petrol.

Many of these and other comparable incidents have common factors:

- **Information Leakage**: Often, attackers have prior knowledge or suspicion about the victim's crypto holdings.
- **Diverse Tactics**: Ranging from SWATting, kidnapping, to straightforward robberies or home invasions.
- **High Stakes**: The attackers are motivated by the potential for significant financial gain from crypto assets.
- **High Risk of physical harm to victims**: Victims and their families are frequently subjected to actual and/or threatened physical violence during an attack.

In short, it is our firm view that the extent of the information-gathering and information retention requirements imposed by the Regulations and by CARF are not a proportional invasion of privacy, particularly given that every user of a cryptoasset exchange already undergoes appropriate KYC and AML checks. These requirements are in particular not proportional given the extent of the extreme risks of violence imposed on individual users and the consequential risks to their right to privacy and family life supposedly ensured by Article 8 of the Convention. As we have demonstrated above, it is reasonable to assume that information which is gathered and retained is likely at some stage to be accessed by or exposed to bad actors. The more parties with whom this information is shared, the

greater the risk. As we have shown, once such information is accessed it is relatively trivial for a bad actor to determine how much Bitcoin a person holds, how often they have transacted, and the addresses which that person currently controls. With the additional knowledge of that person's physical location or home address, and the fact that, once transferred, stolen Bitcoin cannot be frozen or easily recovered, it is not unreasonable to conclude that the risks imposed by the current iteration of the Regulations are unacceptable.

HMG still has the chance to be forward thinking in its implementation and in striking a balance between wanting disclosures on the one hand in order to provide HMRC with relevant information, and its duty as a Government to protect its citizens on the other. As drafted, the Regulation creates a risk of harm for law-abiding citizens that no government should contemplate.

RECOMMENDATION: We strongly recommend that the extent of the information-gathering requirements included in CARF are revisited by HMG when preparing the final draft of the Regulations. Proportionate limitations could include:

(i) limiting disclosures only to those where a user has in one financial year made disposals of crypto-assets that might exceed a material threshold (such as the £200k limit generally relevant for monitoring purposes in an income tax context), and then only retaining that information for a limited period (such as three tax years or less);

(ii) ensuring that *de minimis* levels are set appropriately, as per the US implementation of the Travel Rule, thus reducing both the burden of compliance for a relevant CASP and the risk of wholesale disclosure of a person's crypto-asset holdings following data breaches; and

(iii) not sharing real names and addresses other than in limited circumstances, and never in plain text, unless a user can be shown to have made disposals in excess of the tax-free personal allowance.

Such modifications, while neither foolproof nor exhaustive, may go some way towards mitigating the otherwise considerable risks of harm to UK taxpayers imposed by the Regulations as currently drafted. We note that ensuring tax compliance in the sphere of decentralized and peer to peer monetary networks is challenging, but while making this concession our view remains that the risks to privacy and personal safety posed by the extent of the personal data collection and retention required by CARF and the Regulations outweigh these legitimate concerns.