Prime Minister of the UK
And First Lord of the Treasury
The Rt Hon Rishi Sunak MP
Cabinet Office
70 Whitehall
London
SW1A 2AS
United Kingdom

Foundation Human Rights in Finance.EU
legal@hrif.eu
Amsterdam

August 26, 2023

Dear Mr Sunak,

Our organisation, Human Rights in Finance.EU, and its founder/board member Simon Lelieveldt have been active on the subject of protecting human rights in Finance since before the Brexit. Our objective is to pro-actively protect and shield citizens, companies and the legal professionals from all kinds of legislation, business and governments acts which unduly infringe on human rights as part of charters and treaties that protect Human Rights and privacy. **In line with this objective, we hereby urgently call upon the UK government to strike out and annul all provisions related to the travel rule in both finance and crypto.**

UK Government violates fundamental human rights through its regulation

One important reason to send you this letter is that, right now, the UK is on the verge of implementing an ill-conceived regulation which does further harm not only to European citizens but also to UK companies. In our view the regulation infringes and is incompatible with the rights to privacy and data protection enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, the principles of necessity of such measures in a democratic society and their proportionality, and the case law of the Court of Justice of the European Union.

By forcing UK companies to violate human rights of its customers (including EU citizens) the UK does the opposite of what is written in the UN Resolution on privacy in a digital age. This resolution (42/15, adopted on 26th of September 2019) calls upon states:

> *(j) To refrain from requiring business enterprises to take steps that interfere with the right to privacy in an arbitrary or unlawful way, and to protect individuals from harm, including that caused by business enterprises through data collection, processing, storage and sharing and profiling, and the use of automated processes and machine learning;*

Revoke the travel rule for finance and refrain from invoking it for crypto in September 2023 !

Our concern lies with the provisions within the Money Laundering Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs) that implement the travel rule for both crypto asset and conventional bank/financial transfers in the UK. This travel rule mandates that transfers of funds and crypto assets include specific identifiable information about the sender and the recipient. Non-compliance can result in fines for crypto asset businesses and financial institutions.

Both the crypto-industry and financial services sector recognize the unnecessary burden posed by the travel rule. Its initial justification was to grant foreign law enforcement agencies easy access to personal data of foreign citizens without the need to establish reasonable suspicion. This process allows local law enforcement authorities to request private data from local companies without adhering to proper due process. A glance at historical government records, particularly those related to 'FATF Special Recommendation VII,' underscores our point:

> *Specifically, it aims to ensure that basic information on the originator of wire transfers is immediately available (1) to appropriate law enforcement and/or prosecutorial authorities to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing the assets of terrorists or other criminals, (2) to financial intelligence units for analysing suspicious or unusual activity and disseminating it as necessary, and (3) to beneficiary financial institutions to facilitate the identification and reporting of suspicious transactions.*

It's noteworthy that throughout its decades-long existence, the travel rule has never undergone scrutiny to assess its practical effectiveness. However, its costs are substantial. The rule necessitates the widespread sharing of private data and places an obligation on companies to oversee one another, ensuring that necessary information is included in messages (or sent later for crypto transactions). Despite these immense costs, the benefits of such actions remain unproven and unassessed.

Disproportionality: unnecessary sharing of private data of all innocent people

While the travel rule incurs substantial costs and implementation efforts, it fails to provide any tangible risk mitigation or control measures for the individual companies compelled to adhere to it as a sending entity and police their business partners at the receiving end. Effectively, it operates as a 'comply without question' directive, framed within a broader anti-money laundering and anti-terrorist financing framework. This requirement is driven solely by the obligation to execute it, holding no practical value for legitimate companies genuinely concerned about customer data minimization and welfare. It's worth noting that aside from the travel rule, stipulations are in place which still allow prompt access to personal data to any law enforcement officer with legitimate grounds, proper authority, and evidence of suspicion related to money laundering or terrorist financing.

The redundant character of this rule has received unequivocal acknowledgment from stakeholders across the finance and crypto industries. However, governments find themselves constrained by the Financial Action Task Force (FATF), which, in tandem with covert U.S. diplomatic influences, coerces nations to comply with its 'recommendations' through an intricate mechanism of peer pressure. To shed light on the comprehensive array of driving forces propelling the swift adoption of the crypto-asset travel rule in the UK, we intend to submit a separate freedom of information request to your government.

In every respect, it becomes evident that the implementation of the crypto travel rule occurs within a vastly different context compared to that of the traditional financial sector. Beneficiary recipients operate under disparate regulatory frameworks, and some may not even be regulated at all. It raises a perplexing question: how can a rule of this nature feasibly extend to cover self-hosted wallets? It's akin to imposing AML regulations and data documentation requirements on banknotes within the wallets of ordinary citizens.

Adding to the complexity, governments across the globe have faltered in establishing effective regulations and enforcing consequences against blatant violators in the cryptocurrency sphere. As an illustrative example, in the Netherlands, the process of ousting the largest illicit provider of cryptocurrency services consumed over three years. This transpired despite the market and observers having clear evidence of their violation of AML laws and GDPR regulations since May 2020. Beneficiairy institutions may well be illegal and or dishonest.

Of utmost significance, however, is the shift in the data protection landscape since the days of Special Recommendation VII. A protracted debate and legal saga (comprising Schrems I, II, and III) is presently underway, challenging the legality and adequacy of data protection for EU citizens' information within non-EU jurisdictions. Notably, it's essential to recognize that newspapers and scholars have documented a pivotal instance: within a mere two weeks post the 9/11 attack, the US government had initiated surveillance of SWIFT data on its soil[1].

This manoeuvre catered to the insatiable US appetite for extensive data collection, aimed at identifying every party involved in economic transactions. It is no surprise that when the US in 2018 provided the chairmanship of the OECD-assisted working group 'Financial Action Task Force', it also wished to extend this data collection rule to crypto-assets in order to maintain their stronghold/view on the economic data processes without due authority or any suspicion. We rest assured our Freedom of Information request will shed more light on those dynamics, as a similar request in the Netherlands demonstrated the US ambassador visiting the Ministry of Finance to underscore the importance of this topic.

It stands out as remarkable that, in spite of the remarkable technological progress and the strides made in legal frameworks for data protection across global jurisdictions, no government has undertaken the essential step of revisiting the drawing board to discard the travel rule as superfluous. Scientist did however (C. Kaiser), and to them it is evident that this rule starkly transgresses the foundational principles of data minimization, particularly within a legal context where access to data is readily attainable upon establishment of a suspicion of criminal activity. The situation appears to disregard the existence of UN resolutions addressing privacy in the digital era, landmark decisions by the EU Court of Justice regarding data retention, and the overarching principles outlined in the UK-GDPR (article 5.1 b/c/f).

Outdated public private partnership for undue mass data distribution

The travel rule emerges as an obligation rooted in a bygone era, where regulations and enforcement methodologies were conceived under the premise of private entities being compelled to collaborate with law enforcement agencies. These public-private partnerships blur the distinct constitutional roles of these actors and ultimately operate to the detriment of citizens' civil rights.

While government entities are held accountable to international standards and treaties, individual companies operating under these treaties remain immune from challenge. Consequently, the travel rule's impact rests in the fact that governments, devoid of the constitutional mandate to gather and disseminate such data without substantial suspicion of relevant criminal activities, effectively delegate this function to companies. This action effectively outsources human rights violations to the private sector.

[1] Bank Data Is Sifted by U.S. in Secret to Block Terror, Eric Lichtblau and James Risen, The New York Times, June 23, 2006.

UK companies forced into violating human rights with the UK travel rule

The travel rule obligations place UK companies in an untenable predicament. They are compelled to fulfil a data export requirement that not only lacks utility but also has the potential to harm their clientele. This obligation necessitates transmitting customer data to their competitors—an action that leaves companies liable for any ensuing damages. Additionally, the UK government shares responsibility, as the potential for abuse of this regulation, due to its non-adherence to data minimization and human rights principles, is easy to anticipate (as detailed below).

Our foundation is keen to understand how the UK government reconciles the anticipated crypto-travel rule (as well as the current rule for financial transactions) with the Guiding Principles for Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework (HR/PUB/11/04), endorsed on June 16, 2011, in the Human Rights Council:

> *These Guiding Principles are grounded in recognition of:*
> *(a) States' existing obligations to respect, protect and fulfil human rights and fundamental freedoms;*
> *(b) The role of business enterprises as specialized organs of society performing specialized functions, required to comply with all applicable laws and to respect human rights;*
> *(c) The need for rights and obligations to be matched to appropriate and effective remedies when breached. These Guiding Principles apply to all States and to all business enterprises, both transnational and others, regardless of their size, sector, location, ownership and structure*

For companies the Framework establishes the following:

> *11. Business enterprises should respect human rights. This means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved.*
>
> *12. The responsibility of business enterprises to respect human rights refers to internationally recognized human rights – understood, at a minimum, as those expressed in the International Bill of Human Rights and the principles concerning fundamental rights set out in the International Labour Organization's Declaration on Fundamental Principles and Rights at Work.*
>
> *13. The responsibility to respect human rights requires that business enterprises:*
> *(a) Avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur;*
> *(b) Seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts.*

Our foundation arrives at the inevitable conclusion that UK companies are faced with a challenging decision—to determine which laws to contravene. Should they prioritize upholding human rights and refrain from implementing the travel rule (for crypto), awaiting more definitive clarity on their constitutional soundness within the framework of human rights treaties? Alternatively, will apprehension of punitive fines lead them to transgress human rights principles in order to avoid financial penalties?

The potential for abuse in both individual and widespread contexts is alarming.
Consider a scenario involving a refugee family from country A, currently residing in the UK. They intend to support an ongoing conflict in their home country by sending cryptocurrency to an address operated by a provider in another nation. Unbeknownst to them, this crypto-address is a deceptive ploy orchestrated by government A. Consequently, the sender's name, complete address, full identification details, and possibly even their birthplace—facilitating ethnic profiling—are now at the disposal of government A. Is the UK government willing to subject refugees within its borders to such risks? Similarly, does the government endorse exposing anyone conducting a credit transfer to such risks?

The malleability of the wording and definition of a crypto asset, allows for the convenient creation of a system where specific customer actions—such as purchasing theatre tickets or logging into websites—are conducted using crypto assets as access tokens. Now envision a scenario where a platform like Facebook employs crypto assets for user login. In this context, the UK government appears to be providing such entities an unobstructed and legalised path to globally disseminate its most valuable customer data across various branches, all justified under the pretext of averting money laundering. Our question: are the data protection standards upheld in all these recipient countries as stringently as they are in the UK?

We call upon UK companies to not implement the travel rule and its update
We earnestly urge UK companies to abstain from adopting the travel rule and its subsequent updates. Historically, businesses have often opted to infringe upon human rights, as Data Protection Authorities are understaffed and the complexity of the subject matter hampers thorough understanding. Conversely, AML supervisors exhibit eagerness in imposing fines for even minor legal breaches, and consumers lack the financial means to engage with this intricate subject. This imbalance swiftly tilts against the preservation of human rights. This is precisely where our foundation steps in.

In order to evade legal accountability for potential repercussions arising from their actions, our foundation strongly advises these companies against implementing the travel rule. We are fully prepared to offer our insights and assistance to these companies. It's worth noting that one of our founders successfully compelled the financial supervisor in the Netherlands, through litigation, to revoke an unlawful AML requirement linked to the travel rule.

Furthermore, we wish to emphasize that we will not hesitate to explore the possibility of initiating formal litigation against UK companies that intend to implement the travel rule—be it within the realm of cryptocurrency or in the conventional financial sector.

Annul the travel rule for finance and do not implement it for crypto
We respectfully implore the UK Government to reevaluate its present course of action and to harmonize its regulatory measures with the fundamental tenets of human rights and privacy.

Thank you for your attention to this critical matter.
With kind regards,

Simon Lelieveldt
Board of Foundation Human Rights in Finance.EU
Contact: legal@hrif.eu (digital version of letter)