

Submissions to the DRCF's 2023/24 Workplan – Call for Input

Content

1. [Advertising Standards Authority \(ASA\)](#)
2. [Callsign UK Ltd](#)
3. [Carnegie UK](#)
4. [Centre for Information Policy Leadership \(CIPL\)](#)
5. [Chainalysis](#)
6. [Coventry University](#)

1. Advertising Standards Authority (ASA)

Non-Fungible Tokens

Introduction

The ASA, as the UK's independent advertising regulator, has been administering the non-broadcast advertising code for 60 years and the broadcast advertising code for 18 years. Our work includes undertaking proactive projects as well as acting on complaints to tackle misleading, offensive or harmful adverts.

As the UK's frontline advertising regulator, the ASA brings together different statutory, co-regulatory and self-regulatory enforcement mechanisms so they appear seamless to people and businesses. Our system involves the active participation of a range of legal backstops in the consumer protection landscape. We work closely with a network of partners including the Gambling Commission, the Information Commissioner's Office, the Financial Conduct Authority and the Competition and Markets Authority.

We use our convening powers to bring together the ad industry and media owners to set, maintain and police high standards. Through the sharing of information, joined-up enforcement action and referral processes, our partners bolster our regulation and assist us, where necessary, to bring noncompliant advertisers into line. Together, this 'collective regulation' helps to protect people and responsible businesses from irresponsible ads: ads that mislead, harm or offend their audience.

The ASA is concerned about the shifting and growing landscape in the sale of non-fungible tokens (NFTs) and has presented this paper to highlight our concerns and seek the views and support of regulatory partners to create a framework for the advertising of NFTs in the UK.

Our regulation of cryptoasset advertising to date

Cryptoassets are highly volatile, complex products, subject to frequent changes in value, that can potentially lead investors to experience large falls in the value of their cryptoassets which, because most are not currently regulated by the FCA, do not fall under the umbrella of financial compensation schemes such as the Financial Services Compensation Scheme or the Financial Ombudsman. Absence of statutory regulation also means that cryptoasset advertising does not fall under FCA financial promotions rules. We therefore recognise the important role we play in regulating ads for cryptoassets to ensure they do not mislead consumers about a product's risks or act irresponsibly in their promotion.

In recent years, in and around the pandemic, we witnessed a significant increase in the volume of ads for cryptocurrencies, with the increase particularly noticeable for online media. Given the high risk of consumer detriment, in 2021 the ASA identified cryptocurrency advertising as a

‘red alert’ priority, and we took the decision to proactively investigate selected cryptocurrency ads across different online media to act as precedent-setting cases that would establish the ground-rules for advertising. Twelve rulings were published in late December 2021 to ensure widespread media impact and to bring to the attention of consumers the risks involved with cryptocurrencies. We followed that with an Enforcement Notice sent to 50 cryptoasset companies in March 2022. Since then we have been actively monitoring the market for problematic cryptocurrency advertising using AI tools to assist us and, to date, have seen a significant improvement in compliance. Prior to the Enforcement Notice, all in-remit ads for six key advertisers (identified as accounting for the vast majority of ads in the UK) were found to be non-compliant before the Enforcement Notice, particularly for posters and the Meta ad library. However, except for a single Twitter bio, total compliance was seen across all media after the Enforcement Notice, including for Crypto.com, the most prolific but least compliant advertiser at the start of enforcement.

Non-Fungible Tokens (NFTs), as a type of cryptoasset, are also unregulated and highly volatile in value, and therefore present similar – but not identical – risks to consumers. Last year saw an explosion in both the popularity and advertising of NFTs, with the surge in interest primarily from their presence in the world of collectibles and digital art, collaboration with noted celebrities or sportspeople and the media attention surrounding the sale of particular NFTs at auction for very high prices, sometimes reaching into the millions. The increase in NFT advertising has been particularly noticeable in paid, online media.

We’ve conducted preliminary scoping and have identified several potential issues with current NFT advertising:

- Absence of risk warnings or regulatory status.
- Absence of information about applicable fees unlikely to be known to consumers, for example gas fees, platform commission/service charges and smart contract-embedded royalty fees on future sales.
- Absence of information relating to ownership rights or significant restrictions on the use/resale of the NFT.
- Exaggerated claims about the value or future performance of NFTs.
- Ads trivialising an investment or potentially taking advantage of consumers’ inexperience, particularly when targeted at the social media followers of celebrities or sportspeople likely to be unfamiliar with NFT purchase and resale.
- Targeting of NFT ads to children.
- Implied “fear of missing out” claims.

Examples of NFT ads reflecting some of these issues are provided in the appendix.

Given the potential for consumer detriment, we are conducting a similar proactive approach to that for cryptocurrency and have already begun three investigations into ads that unambiguously promote NFTs as investments. The subsequent rulings (due later this year) should set out some basic principles for NFT advertising with respect to risk warnings, regulatory and performance information.

However, unlike cryptocurrency, there is arguably a greater level of complexity and nuance associated with NFTs that merits wider consideration. We would welcome views from other regulatory partners, both to benefit from a range of expert views and to work towards comprehensive, complementary and consistent regulation of NFT ads.

Factors influencing the regulation of NFT advertising

NFTs can serve different functions depending on the context. Some are explicitly presented for their investment potential, others are positioned as a form of receipt of ownership on a blockchain, others are promoted as collectibles for sports fans, others as a form of hobby purchase. That said, some NFTs contain multiple features. For instance, collectible NFTs that are also promoted as having investment potential. It might be said that the purpose of NFTs can exist along a range of benefits from pure investment purpose at one end of the scale to that of hobby/collectible at the other.

NFTs are also becoming more prevalent for purchase within gaming or have other utility functions, while NFTs are also being used to raise money for charitable causes. More recently, NFTs have been finding their way into the property market, both digital and 'real-world'.

This means that, compared to cryptocurrency, a one-size-fits-all approach to the regulation of NFT advertising is arguably less feasible for a number of reasons.

Are NFTs always an investment product?

We're aware of discussions amongst industry stakeholders and the media about whether it is reasonable to consider that an NFT is being marketed as an investment product in all circumstances, particularly in the absence of any implied or explicit investment terminology. However, we also note that regardless of the context in which an NFT is promoted, in most circumstances consumers need to have a digital wallet funded with cryptocurrency, which may potentially expose them to further risk.

Any decision would be likely to influence the requirements we put in place for NFT advertising, for example:

- Whether all NFT ads should make clear that they are a form of cryptoasset which is unregulated and highly volatile, as we require for cryptocurrency ads.

- How we regard the responsibility of NFT ads with content that may target, or appeal to children, or responsibility concerns more generally.
- How we apply our rules to NFTs advertised for charitable purposes.
- How our rules are applied to ads for competitions or promotions including NFTs.

In considering this matter, we also understand that while the government determined that qualifying cryptoassets are brought under the Financial Promotion Order, non-fungible tokens have been left out of scope. HM Treasury's Cryptoasset Promotions consultation response explains that "non-fungible tokens may represent a wide array of different assets which might constitute non-financial services products. Additionally, as the non-fungible token market is evolving rapidly and remains at an early stage of development, the government does not yet have sufficient information on risks and use-cases. As such, seeking to bring non-fungible tokens into scope might have unintended consequences for the market".

Adding to this complexity we are also aware of the emergence of 'fractional NFTs', where an NFT is split into a number of equivalent tokens for purchase by multiple owners which are tradable. We understand that in this scenario a fractional NFT would constitute a fungible token and as such, could then impact whether ads for fractional NFTs would come under the Financial Promotions Order.

We are therefore mindful that any decisions we make concerning the presentation of NFTs as investments may raise potential conflict with a statutory view.

Money Laundering Regulations

Businesses that undertake certain cryptoasset activity in the UK are required to register with the FCA for money laundering supervision. Our previous enforcement work on cryptocurrency advertising identified ads for some businesses that undertake cryptoasset activity without the required authorisation and which are therefore operating illegally. As such, we refer ads for these companies to the FCA for follow-up. It is not clear whether firms providing NFTs would require similar registration, but if so would impact on our enforcement capability for such advertising.

Capital Gains Tax and other taxes

The ASA requires that cryptocurrency ads include a statement that Capital Gains Tax may apply to transactions, based on HMRC guidance. Although we understand NFTs are likely to be treated as taxable assets for capital gains and inheritance tax purposes, we note that no formal guidance for NFTs has yet been published by HMRC, so it is unclear whether the same disclosure should be required for NFT advertising.

Legislative implications

As an emerging technology, NFTs incorporate features that raise questions about the application of existing legislation. In July, the Law Commission published a consultation paper¹ which includes discussion of NFTs in relation to legislation relating to matters such as intellectual property rights, licensing, copyright, smart contracts and royalties, as well as a recent project², sponsored by the Ministry of Justice, to consider the private international law challenges in tech-related disputes, both with a view to provide clarity in areas of legal uncertainty and to suggest reforms.

As a non-statutory body, the ASA does not enforce legislation, but our Codes are developed to work within and to complement legal controls. Legislative changes may therefore impact our Codes and how we interpret and apply our rules to NFT ads, particularly in matters relating to material information, pricing, and the use of data for marketing. We are also mindful of the fact that the technology behind NFTs is complex and terms and conditions relating to purchase, ownership rights and transfer may be more difficult for consumers to understand. As well as having responsibility for how these are presented on websites advertising NFTs that fall within our remit, we also need to consider which conditions are so significant that they warrant inclusion on both paid-for ads and social media ads.

NFTs and gambling

NFTs have found their way onto online gambling platforms, and can be incorporated into casinos, sport and esports betting. We understand that the Gambling Commission has taken an interest in several NFT-based services in relation to whether they may constitute an illegal lottery, or alternatively, whether they are an unlicensed gambling platform. In reference to NFTs, Andrew Rhodes³, Gambling Commission CEO, recently acknowledged that the boundaries of what can be defined and regulated as gambling products are becoming increasingly blurred.

Government NFTs

Earlier in the year, the then Chancellor of the Exchequer announced that the Royal Mint will create and release a range of NFTs in summer 2022, as part of the UK's 'forward-looking approach' towards cryptoassets. The release of the NFTs is now uncertain under the new Government, but we still need to consider whether these government proposals provide credibility for NFTs that has implications for regulatory provision.

¹ Law Commission: Digital assets consultation paper <https://www.lawcom.gov.uk/project/digital-assets/>

² Law Commission: Digital assets: which law, which court? <https://www.lawcom.gov.uk/law-commission-review-to-examine-how-private-international-law-can-apply-to-digital-assets-and-other-emerging-technology/>

³ IAGR Conference 2022: <https://www.gamblingcommission.gov.uk/news/article/andrew-rhodes-speech-at-iagr-conference-2022>

Enforcement challenges

When rules have been put in place for NFT ads, they need to be enforced across the industry. However, compared to cryptocurrency, enforcement of NFT ads is more difficult for several reasons:

- **Range of NFT providers:** Compared to cryptocurrency ads which are primarily placed by a relatively small number of cryptocurrency firms or exchanges, NFTs may be sold by a large variety of retailers including cryptoasset firms, NFT marketplaces, sports teams, fashion retailers, jewellers, musicians, artists and museums. The barriers to entry to market are very low, so anyone can, if they wish, go online, “mint” and then market their own NFT. Distribution of guidance and effective enforcement action across such a large range of industries and providers is therefore going to be much more difficult.
- **Scams:** ASA intelligence suggests that NFTs are an attractive mechanism for scams by criminal actors. A well-known NFT-related scam is a ‘rug pull’, where developers set up an NFT project, drive up the price through promotional hype, sell their NFTs, then suddenly stop backing it, plunging its value to zero. There may be difficulties in identifying which ads are for legitimate or scam NFTs and how to regulate across these two scenarios.
- **Identification and location of providers:** Whilst some NFT providers and advertisers are UK-based, a large number are based overseas yet targeting the UK market through their partnerships (with sports stars for example) or their direct promotional activity. In other cases, it may be difficult to determine where an NFT provider is based or even the legal entity behind an NFT ad. This may have implications for regulatory remit and enforcement action. Advertising of NFTs within the metaverse is also likely to raise issues relating to regulatory jurisdiction.

Conclusion and discussion points

NFTs are a complex product which present risks and issues which are not the sole concern of advertising regulation. Decisions need to take a number of factors into account and require discussion with other interested regulators and stakeholders to ensure that the resulting framework for the marketing of NFTs is robust and aligned with statutory views.

We are aware that the DRCF works to promote coherence between regimes, collaboration and building of capability across regulators, and the ASA believes that this is particularly key to ensure effective regulation of NFTs. We therefore ask whether the DRCF can consider this paper.

In doing so, and as a starting point, we have suggested some discussion points on the following points of principle:

1. Given the fact that all NFTs are a form of cryptoasset and all require consumers to open a cryptocurrency account, and mindful of the risks that cryptoassets pose to UK consumers, the ASA is minded (through its current ongoing investigations) to put in place rules that will require all NFTs ads to disclose:
 - That NFTs are a form of cryptoasset
 - That they are unregulated by UK financial authorities
 - That they are volatile

2. As a matter of public policy such a position will prevent NFT advertising from appearing on mainstream UK broadcast channels. It would also circumvent the issue outlined above concerning how NFTs can be considered along a spectrum from hobby to investment. We believe that this is in the consumer interest given the risks that cryptoassets pose to UK consumers, but we would welcome others' views.

3. Clarification on the tax treatment of NFTs is in the interests of UK consumers so it can be reflected in the information required in NFT advertising. HMRC should be encouraged to provide certainty of tax treatment of NFTs as a matter of priority.

4. We are also keen to discuss the position of statutory regulators on NFTs and any impending changes that may impact on our requirements for, and subsequent enforcement of, NFT ads, particularly in relation to:
 - Application of Money Laundering Regulations to NFT providers.
 - Consideration of fractional NFTs as a fungible token and impact on future financial
 - promotion requirements.
 - Best practice presentation of NFT-specific terms and conditions to consumers,
 - particularly relating to smart contracts, pricing, IP rights and licensing matters.

5. Finally, we ask whether there is any interest in maintaining regular communication on NFT matters to ensure consistency and robust regulation. We note that in recent days the Department for Culture, Media and Sport has announced an enquiry into NFTs; so, partner regulators may wish to co-ordinate and collaborate on responses.

Other policy interactions and technologies we would like the DRCF to take into consideration as it develops its workplan for 2023/24

As part of the ASA's five-year strategy, More Impact Online, we are harnessing technology to help us regulate advertising online more effectively. Using avatar technology (online profiles which simulate children's browsing activity), web scraping tools and mobile phone metering software we are monitoring age-restricted ads to identify the minority that, in breach of our rules, are placed on websites disproportionately popular with children or that are served to the social media accounts of children who are age-registered as 17 or younger. This has been followed by effective follow-up enforcement action.

We have also worked closely with online platforms to lift the lid on alcohol marketers' audience-targeting selections, to help us understand whether they are taking appropriate steps to target their ads to an adult audience and away from a child audience in logged-in social media environments. In a landmark project, between 1 February 2020 and 31 March 2020, Facebook, Instagram, Snapchat, Twitter and YouTube submitted brand-anonymised targeting data to the ASA relating to over 2,000 alcohol campaigns run on these platforms. This work recognised that platforms, which play an important role in children's lives, are significant repositories of marketing data, including brands' targeting practices, which – for the purpose of this project – they anonymised and shared with us. By sharing the anonymised data with us, the platforms helped us to uncover important insights into the extent to which alcohol brands and their agencies are using the tools available to them (which differ from platform to platform) to target their ads away from children's social media accounts.

Last year, in a world first, in collaboration with the largest companies in the digital advertising supply chain (Adform, Amazon Ads, Google, Index Exchange, Magnite, Meta, Snap Inc., TikTok, Twitter and Yahoo), we launched a pilot, which extends the ASA's role online. Under the title of 'Intermediary and Platform Principles', the pilot explores the merits of formalising and bringing more accountability and transparency to the role that these companies play in helping to uphold the UK's world-leading system of advertising regulation. As part of the pilot, participating companies voluntarily agree to provide information to us to demonstrate how they operate in accordance with the pilot's principles.

As DRCF develops its workplan we believe it is important it considers looking at ways of improving transparency and data sharing by digital platforms; of particular relevance to the work of the ASA, it is increasingly important that we have access to online ad data (e.g. ad creative and ad media placement; age / potential vulnerabilities of audience in receipt of particular ads; marketers' use of known/inferred data for the purposes of ad targeting; etc.) in order to support independent ad monitoring activities and inform our regulatory interventions. This relates to banner ads, in-feed ads, pop-up ads and other ads in traditional paid-space online; organic ads (in brands' owned media) and influencer ads. We imagine that the need for data transparency and data access is relevant, and currently presents a challenge to, all DRCF members.

A separate point, we also think DRCF should bring or keep algorithm design under consideration. We know from discussions with civil servants (in the context of body image related harms) that there are concerns around how the use of algorithms can have negative impacts on young social media users; with online platforms tending to serve more and more content that could have a potentially harmful psychological impact.

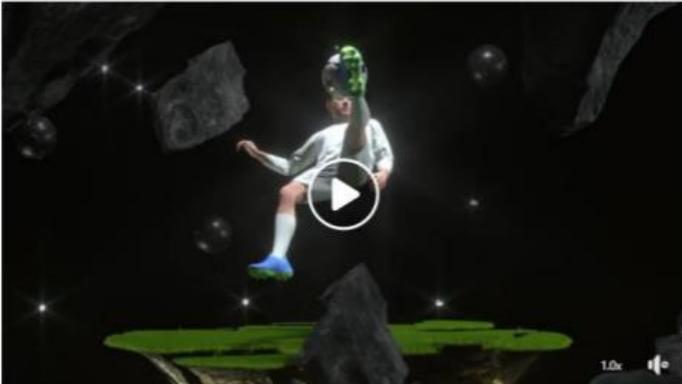
To the best of our understanding, we aren't aware of any particular policy thinking around this in the online safety bill. It's conceivable that the requirements in the UK Online Safety bill around platforms providing tools to help people see less of certain types of content could

include consideration of algorithms but it doesn't necessarily follow. While this seems more of a media regulatory issue (Ofcom?), advertising also involves a lot of algorithmic processes. We can conceive of a shared interest between Ofcom and the ICO on this issue.

Appendix: Examples of NFT advertising

Crypto.com Sponsored

Gareth Bale is a celebrated footballer who plays for Real Madrid and serves as the captain of the Welsh national team. Together with London-based artist DINES, Bale dropped a 4-piece collection featuring digitally-signed trading cards that commemorate the greatest moments of his stellar career so far. Explore pieces from "Gareth Bale: The Evolution of a Footballer" by signing up to [Crypto.com/NFT](https://crypto.com/NFT) now!



CRYPTO.COM
Crypto.com NFT | Buy, Sell, Discover Exclusive Digital Collectibles Sign up

Crypto.com Sponsored

AstonMartinF1 is back with the AMR22 NFT collection (Live for 48 hours!)

This collection celebrates AMR22, representing the biggest design overhaul in Aston Martin Formula One history.

Collect NFTs from "AMR22" to unlock exclusive prizes, suc...



Ad - <https://www.sorare.com/football/nft>

Sorare - Fantasy Football - Collectible Football NFTs - sorare.com

A new fantasy **football** game is in town, buy, trade and play with official digital cards! Collect the best players, compete across multiple divisions, win exclusive prizes weekly.

Game Rules

- Collectible digital cards
- Tracking real performances

Licensed Clubs

- More than 200 clubs
- Greatest leagues in the world

GetintheGoal @GetintheGoal1 · Dec 8
Football NFTs are here

Get in early and trade through 2022. Before the boom.

Search for GetintheGoal on #rarible

#NFT #rarible #collectibles #digitalcollectibles #footballnft #soccernft #soccercollectibles #liverpoolnft #afc #chelseaNFT #chelsea #leicesterNFT #evertonNFT

Search for GetintheGoal on: RARIBLE, OpenSea, M

Warrington Wolves @WarringtonRLFC · Nov 11
Rugby League's first ever NFTs: Dropped

Be the owner of one of seven George Williams collectible non-fungible tokens: www.wolves.com/NFT

0:16 10.2K views

Metaboys
Sponsored

The first NFT that creates a private club sharing a network of world-class entrepreneurs & investors. Only 7 WL spots left. A-players only.

THIS IS THE BIGGEST NFTS LAUNCH OF 2022. JOIN THEIR DISCORD NOW

Thunder Lands NFT
Sponsored

INVEST, EARN AND BE AHEAD OF THE REST

An innovative Blockchain-based Unreal Engine 5 MMO at the junction of RPG and Strategy.

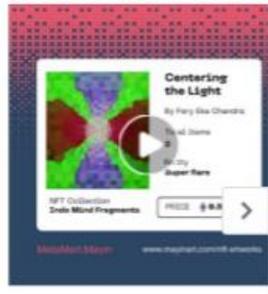
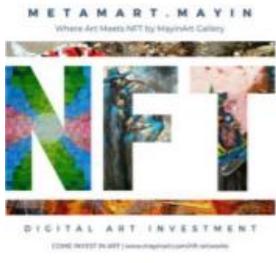
Get whitelisted and join NFT game collection presale before it goes mainstream...

THUNDERLANDS STORE
Get whitelisted now!
Thunder Lands is a virtual gaming metaverse set in the Dark Fantasy genre. Classical gameplay + aspects of innovative...

Sign up



STOP! Do you want to kickstart investments in NFT?
MayinArt's First NFT Collection is LIVE - "Indo Mind Fragments"
MayinArt's NFT gallery, MetaMart.Mayin debuts its first collection, a digitised collection of 10 exclusive paintings by MayinArt's artists now available for NFT enthusiasts to buy!



Nexus.Art is an NFT Platform to democratize the process of buying & selling for musicians, artists & investors. Power to the People.



NEXUS.ART
NFTs Made Over \$10 Billion in 2021 📈
NFTs will truly shift the paradigm & change the world. Join the revolution & claim your piece of history at nexus.art.

Learn more

← Tweet



My Twitter Space is about to go live, to discuss my NFT project. Despite the critics, my NFTs will be the first ever that can't lose their initial value 🙌



Crypto.com
Sponsored

Tattoo artist Jesse Smith's NFT collection is live! 🧡

✉️ The first 5 collectors to own 5 NFTs will win a trip to get a tattoo, with flights + hotel stay!

Sign up to [Crypto.com/NFT](https://crypto.com/NFT) now!



Luke Shaw with Sportemon Go
Sponsored

Excited to announce that I'm teaming up with @sportemongo, one of the world's leading sports NFT producers, to create my own custom line of digital collectibles!

With my first official collection dropping very soon, I'm giving you the chance to get your hands on one for free! All you need to do is pre-register via the link in my bio!...



Ad · <https://www.womplay.io/nft> ▼

Play Top Games & Win Free NFT - Earn Rare NFTs While Gaming

Play top games & **win** free **NFT** on the ultimate gaming rewards platform for gamers. Play & install mobile games, earn points & convert them easily to valuable rewards.

[Earn Free NFTs](#) · [Get NFT Bonus](#) · [Play with NFTs](#) · [Earn Crypto & NFT](#) · [Play NFT Games](#)



**LACA COMPETITION 2021 WIN AN NFT
NON FUNGIBLE TOKEN!**

£3.00

Win an original digital artwork
"Phalaenopsis #2 by Callum Toy"

The winner will also receive a large format artwork file that can be printed to their desired dimensions. LACA will install the winner's crypto wallet should they not already have one.

To enter the LACA NFT Competition answer the following question below and purchase your entry ticket

On the LACA website, what do the letters TAS stand for?

- Total Artist Services
- Telling Art Stories
- Talking Art Series

Submit

1

ADD TO BASKET

← Tweet

Andy Robertson
@andrewroberta05

So excited to announce that I'm exclusively partnering with one of the world's leading sports NFT producers @sportemongo This will create recurring income for my charity @ar26charity



11:06 am · 21 Oct 2021 · Twitter Web App

MusicArt
Sponsored

uaCharitable NFT

- 1st Edition Charity Release #NTF
- Onchain
- ONLY 100 released by artist James Marsh
- Proceeds go to UNHCR UN Refugee Agency offering protection to Ukraine families fleeing their homes...



JdGraffix @JdGraffix · Sep 20, 2021

1. Hey People, As a few of you know I wanted to do some charity donations, so what im doing is donating 90% of my NFT sales/ any personal graphics projects (last 10% for gas fees) to Muscular Dystrophy UK #charity #donation #NFT #saltama



Duchenne muscular dystrophy is a muscle-wasting condition caused by the lack of a protein called dystrophin. It usually affects only boys.

About 100 boys with Duchenne muscular dystrophy are born in the UK each year and there are about 2,500 boys and young men known to be living with the condition in the UK at any one time. For the general population, the risk of having a child with Duchenne muscular dystrophy is about one in every 3,500-5,000 male births.

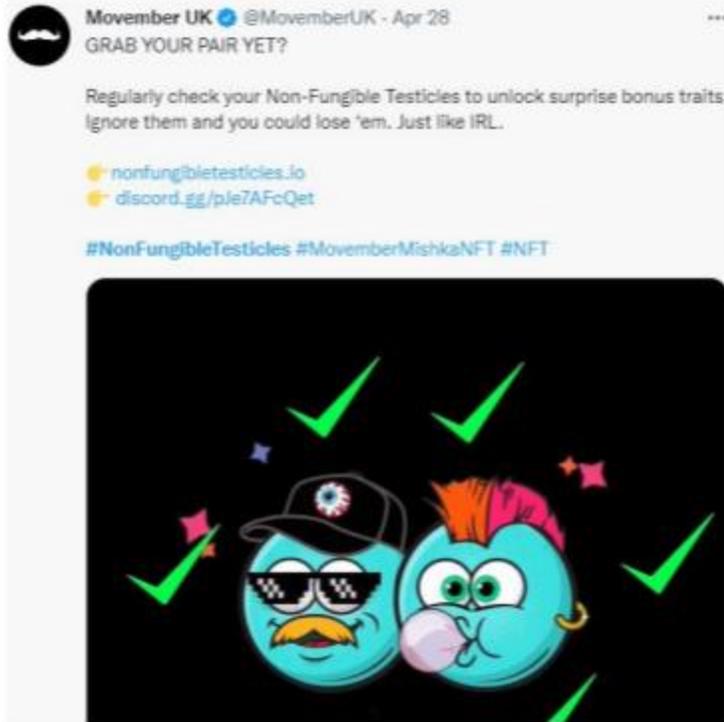
Duchenne muscular dystrophy is a serious condition that causes progressive muscle weakness. Owing to the lack of the dystrophin protein, muscle fibres break down and are replaced by fibrous and or fatty tissue causing the muscle to weaken gradually.

CardanoMan @ADASuperHero · Jan 18

I'm very grateful to align with @grumpybunCNFT. Together, we aim to raise over 10K SADA for UK based animal charities. There is so much money being made in #Crypto and #NFT's and I feel a responsibility to help direct some of that money in a philanthropic direction.



7 13 46



Crypto.com
Sponsored

Kryptomon celebrates its latest in-game update with an exclusive NFT drop 🎁

👑 2,000 Kryptomon eggs are up for grabs, letting you train one from scratch and kickstart your Kryptomon League journey

...



The image is a promotional graphic for 'Kryptomon MYSTERY BOXES'. It features a dark, space-themed background with purple and green accents. In the center, there's a glowing blue and green 'Mystery Box' with a question mark. To the left, a character with purple hair and a pink top looks on. To the right, a green alien-like creature is visible. The text 'Kryptomon' is at the top in pink, and 'MYSTERY BOXES' is in large white letters.

Paul Pogba Retweeted

CryptoDragons.com @CryptoDragons · Dec 23, 2021

Minting Day 🚀 Dec 24
Hatching Day 🌟 Dec 25

🌱 You will finally hatch your Dragons and start 📈

Breeding...❤️
Battling...🗡️
Earning...💰

#nft #nftart #NFTCommunity #cryptodragons



The image is a promotional graphic for 'CryptoDragons.com'. It features a dark purple background with three colorful dragon characters. The text 'CryptoDragons.com' is at the top. Below the dragons, it says 'Mint December 24' and 'Hatching, Battles and Breeding Start December 25'.

Crypto.com
Sponsored

👑 NFT avatar project DAVA and premier blockchain game The Sandbox have collaborated on an exclusive drop

🔥 Hurry, just 50 mystery boxes containing avatars and limited-edition wearables await

Sign up to [Crypto.com/NFT](https://crypto.com/NFT) now!



The image is a promotional graphic for 'DAVA x The Sandbox'. It features a vibrant, colorful background with a stylized character on the left and a checkered pattern on the right. The text 'DAVA x The Sandbox' is in the center, with 'crypto.com' at the bottom.

Crypto.com
Sponsored

Set your reminders, because you won't want to miss this drop.

"The World" is a 5,000 piece collection of oriental landscape paintings by generative artist CSLIM. For this project, he created AI that has learned the data of 80,000 classical works through machine learning...



The image is a promotional graphic for 'The World AI - Your Window To Cutting-Edge AI Masterpieces'. It features a dark background with a stylized head icon containing a brain and gears. The text 'crypto.com | NFT' is in the center, followed by 'Get Yours February 21, 2022' and 'The World AI - Your Window To Cutting-Edge AI Masterpieces' at the bottom.

🔍 What are you looking for?
boohooMAN.com
👤 ❤️ 🏠

NEW IN
CLOTHING
SUMMER SHOP
PLUS & TALL
GOING OUT
SWIM
SHOES & ACCESSORIES
SALE

20% OFF ALL BOOHOO MAN - FREE NEXT DAY DELIVERY
SEE CODE: SALE
DOWNLOAD THE APP TODAY
UNLOCK EXCLUSIVE OFFERS & DISCOUNTS
BOOHOO MAN PROMISE ONLY £5.99
UNLIMITED NEXT DAY DELIVERY FOR A YEAR!

THE NFT COLLECTION

**OUR FIRST EVER NFT
RANGE IS DROPPING**

**HERE'S HOW TO COP IT
BEFORE ANYONE ELSE**

We're used to starting trends, and this is no different. For the first time, an affordable fashion brand is launching an unforgettable line of NFTs, and who could get the virtual ball rolling better than boohooMAN?

We're bringing our freshest threads from reality to NFT, to create a range of boohooMAN fits to hang on your virtual rail. We've got a whole collection on offer, including t-shirts, outerwear, trackuits and hoodies, meaning you can turn your digital wallet into a digital wardrobe in no time. Each item is brand new and completely unique, so once it's gone, it's gone.

Create a metaverse-worthy streetwear fit, or just keep them as a collector: once they're yours, the sky's the limit. It's not enough to look cool in real life anymore - time to take your style into the virtual realm.



2. Callsign

Our comments are in response to Question 1 of the Call for Input:

“Are there policy interactions or technologies you would like the DRCF to take into consideration as it develops its workplan for 2023/24? Why are these important? Please outline areas that cover at least two of the DRCF member regulators’ remits”

There are two areas we would like to highlight for the DRCF to take into consideration:

a) Improving accountability online by verifying genuine users will help protect consumers.

There is limited accountability online when compared to the physical world. By building accountability into the online world, it acts as a deterrent to adverse behaviours including online harassment, social engineering, fraudulent advertising, and fake reviews.

There should be greater responsibility on online businesses to identify their users, and to remove harmful content. Accountability should start with verification that the individual is a real, genuine user. After this, stronger verification and authentication of real users’ identities online allows for harmful content to be associated with specific user profiles, and the content to be more easily moderated and removed when perpetrators are identified.

Verifying the genuine user is also essential for solving online challenges such as age verification and the identification of vulnerable customers e.g., in the gambling sector.

In addition to being verified at the point of initial user account creation, users should be subject to robust ongoing authentication, to make sure they are who they say they are when interacting with digital services.

We welcome the work of Ofcom to date on these topics in the Online Safety Bill, as well as the work of the CMA on fake reviews. We note there are UK Government initiatives looking at similar themes, including the Home Office’s Cyber Duty to Protect programme and elements of DCMS’s Digital Identity Programme.

Regulators should encourage the use of innovative, readily available, and easy to deploy technologies to tackle these issues. Technologies in this area are constantly advancing and any solutions deployed must be able to adapt to new threats as they evolve, in order to keep up with the tactics of bad actors and those seeking to cause harm online.

New, innovative technologies such as behavioural biometrics provide a means of authenticating users online in a frictionless way without impacting the customer experience and are already deployed in sectors such as financial services where behavioural biometrics are used for Strong Customer Authentication (SCA) under the Payment Services Directive 2 (PSD2).

Regulators should continue to work collaboratively with industry participants to tackle these issues. We would welcome the opportunity to engage on these topics.

- b) We encourage the FCA to review and consider alignment with the European Banking Authority [EBA] interpretation of the ‘inherence’ element of Strong Customer Authentication (SCA) in the Regulatory Technical Standards on strong customer authentication and secure communication under Payment Services Directive 2 (PSD2) to enhance fraud prevention. Transaction monitoring cannot be used as a substitute for positively asserting the identity of a genuine user, when tackling payment fraud.**

It is encouraging to see the UK financial services industry, under direction of the FCA, taking positive measures to combat fraud. To stay one step ahead of fraudsters, the sector’s approach to fraud prevention must be robust and able to keep up with constantly evolving fraud tactics.

As the FCA is aware, SCA was introduced by the EBA as a way for banks, e-commerce businesses and payment service providers in the European Union to tackle fraud and confirm that an individual is legitimately accessing their bank account or making a transaction.

In November 2021, the FCA extended the definition of the ‘inherence’ element of SCA from relating ‘to physical properties of body parts, physiological characteristics and behavioural processes created by the body, and any combination of these’ to a broader definition that includes behavioural analytics such as spending patterns.

This position diverges from the EBA’s interpretation of ‘inherence’. The EBA clarified in their June 2022 opinion that while “some market participants argued that behavioural characteristics related to the environmental analysis and payment habits, such as those related to location of the PSU, time of transaction, device being used, spending habits, online store where the purchase is carried out, should qualify as inherence... These behavioural characteristics do not relate to a physical property of the body and thus cannot be considered as an inherence SCA element”.

While the types of behavioural analytics noted above can support fraud prevention methods, via transaction analysis, they cannot on their own positively assert the identity of a genuine user is making a transaction.

New, innovative technologies already available in the market, such as behavioural biometrics, offer a method by which ‘inherence’ (as per the EBA’s definition) can be achieved in a seamless manner without impacting the customer experience.

We would encourage the FCA to review and engage with industry on this topic.

Supporting research

Across all industries and the public sector, businesses are realising that digital trust is foundational to success.

Callsign commissioned CEBR to conduct a unique study into the value of digital trust across modern economies.

Callsign's analysis shows that a 1% increase in digital trust drives \$596 increase in GDP per capita. See Callsign's [Digital Trust Index](#).

Businesses must invest in building digital trust. With modern consumers demanding seamless, secure, privacy-preserving and ethical experiences in their digital lives, trust must be built into every digital experience and transaction.

Callsign overview

Founded in 2012, Callsign is a British technology company and a global pioneer in digital identity and fraud prevention. We have developed the first identification platform in the world that uses artificial intelligence to build digital DNA to authenticate users with unparalleled accuracy – right down to the way users type and swipe. Our technology is built on the foundation of privacy, confidentiality, and the protection of user data, with the very highest levels of encryption.

We work with 60% of the UK consumer banking market, helping our clients to authenticate users, meet Strong Customer Authentication (SCA) requirements under PSD2, and tackle social engineering and Authorised Push Payment (APP) scams.

In December 2020, Callsign participated in the FCA and City of London's Digital Sandbox Pilot alongside one of our banking partners to develop our 'dynamic fraud intervention' solution, which aims to reduce APP fraud.

3. Carnegie UK

1. We welcome the opportunity to provide input to the DRCF's workplan for 2023/4. It is good to note that the Forum's objectives are now firmly established and that the plan includes an update on the delivery to date of shared pieces of work. Our main area of focus is on online safety and, as we have set out in our responses to previous DRCF consultations, we are particularly interested in regulatory coherence and the need for regulatory bodies with an interest in the services that will fall under this regime to work closely together. In that regard, we particularly welcomed the very clear statements earlier this year on joint working from the CMA and Ofcom, on managing the links between the digital markets and online safety regimes, and from the ICO and Ofcom, on data and privacy. In the midst of continued delays and uncertainty with the Online Safety Bill, these documents have been very useful to civil society stakeholders like ourselves and, we assume, to industry too as we all seek to look beyond the current Parliamentary process and understand the mechanics required for the successful implementation of the Online Safety Bill, once it receives Royal Assent.
2. We note – and welcome the fact – that “many of the bilateral projects set out in our 2022/23 workplan are envisaged as being multiyear and will therefore be moving into new phases in light of the changing technological and legislative context. For example, the prospect of implementation of new legislative regimes during the 2023/24 period means that DRCF members could be in a more operational phase, highlighting an even greater need for our coherence work.” The delays to the Online Safety Bill, while frustrating for many stakeholders, have at least have the positive consequence of enabling the DRCF's working practices to bed down and to move beyond the hypothetical into some more detailed joint working.

Are there policy interactions or technologies you would like the DRCF to take into consideration as it develops its workplan for 2023/24? Why are these important? Please outline areas that cover at least two of the DRCF member regulators' remits

3. We feel it is important that the DRCF (and specifically the FCA and Ofcom) do not underestimate the scale of the work OSB implementation challenge with regard to the fraud duties and the measures added to the Bill related to fraudulent paidfor advertising. (In light of the Government's recent changes to the OSB to remove the “harms to adults” duties, we are also not entirely sure how advertising that does not fit the narrow definition of fraudulent ads will be dealt with.) Some of the early questions that will need early clarity once the Bill has received Royal Assent include: How are the regulators going to provide oversight? Who's going to “hold the ring” re acting on the findings that come out of Ofcom's lead role eg assessing trends, identifying structural and/or systemic risks, horizon-scanning, analysing the data that comes back from the volumes of evidence that will emerge re fraudsters' online tactics etc? Can OFCOM use insights from other regulators to trigger investigations and use its own information-gathering powers for audits? The accountability

and information-sharing lines to Government will also be important: Who will the regulators report up to in order to influence wider policymaking and how do the departments with an interest in this (Home Office, DCMS, HM Treasury, National Cyber Security Centre) interact? Which regulator will have the lead stakeholder management role with organisations like CIFAS, Stop Scams UK, etc? How much of this can be worked through “in the open” and consulted upon at an early stage?

Beyond fraud and scams, there are also considerations arising from the OSB re standards, particularly with regard to the impact on competition. Also, there may be issues around effective information-gathering and data sharing between the regulators and upwards to sponsoring Government department(s) – can these be worked through now? Will the safety steps required under the OSB impact on data protection requirements, not just in relation to age verification and the AgeAppropriate Design Code for children but also wider account verification? For example, will dominant platforms use sign-on for account verification as a way into other services in order to maintain control over users’ data?

In line with the ‘factors we consider when prioritising work’, are there any areas of focus you believe align with these that are not covered in our previous workplan?

4. We recognise the scale and breadth of the collaborative work already in train in relation to both the implementation of the VSP and online safety regimes and the imminent regulatory requirements arising from the Digital Markets, Competition and Consumer Bill. That said, horizon-scanning and future-proofing work will remain critical as these regimes bed down and mechanisms for the DRCF to continue to undertake shared evidence-gathering and rapid identification of areas of emerging harm will be vital in order to ensure the OSB framework is fit for purpose and reflected in Ofcom’s development of codes and guidance for regulated services in the years ahead

Are there any particular stakeholder groups (e.g. end users such as vulnerable consumers, children, businesses) that you believe the DRCF should be particularly mindful of when prioritising areas of focus for the DRCF?

5. We have a particular interest at Carnegie UK in how the OSB regime will address violence against women and girls and have developed a code of practice⁴ which we believe should be attached to the Online Safety Bill in order to address systemic issues that create harm for women and girls, beyond individual criminal offences (such as those recently signalled by the Government for addition to the OSB). Regardless of the final policy decision on the inclusion of this code in the Bill, hearing directly from victims’ groups - such as those who campaign to stop VAWG – should be an important part of the DRCF’s stakeholder engagement strategy going forward; for example, to inform their horizon-scanning and

⁴ [VAWG-Code-of-Practice-16.05.22-Final-1.pdf \(d1ssu070pg2v9i.cloudfront.net\)](#)



evidence-gathering work re the impact of, and shared risks arising from, the interrelated regulatory frameworks they oversee.

Carnegie UK
December 2022

4. Centre for Information Policy Leadership (CIPL)

i. Introduction

The Centre for Information Policy Leadership (CIPL⁵) welcomes the opportunity to provide input to the Digital Regulation Cooperation Forum (DRCF) workplan 2023 to 2024 by answering to the questions presented in its call.

- i. Are there policy interactions or technologies you would like the DRCF to take into consideration as it develops its workplan for 2023/24? Why are these important? Please outline areas that cover at least two of the DRCF member regulators' remits

Digital Assets in blockchain

Digital assets in blockchain are transforming financial services, both traditional and new, and are taking a foothold in many forms in the an expanding digital economy. As financial services regulators seek to put their arms around this fast evolving area in the US, UK, EU and other jurisdictions, it is imperative that data privacy issues are considered and addressed in tandem with the development of financial services policy and regulation to ensure a coherent, comprehensive and workable regulatory approach, and to support an open, innovative and competitive market in the UK. This interplay is particularly important for the ecosystem in blockchain networks given the foundational role of privacy in establishing and maintaining “trust” in the myriad of financial services innovations being developed. The key elements of blockchain - transparency, immutability, borderless and de-centralised infrastructure – challenge many core concepts of privacy. This needs to be urgently addressed to enable users, providers and the technology and innovation supporting digital assets to continue to innovate with certainty, and to ensure that the UK attracts both talent and investment to be a market leading in digital assets and crypto.

Research published by the UK Financial Conduct Authority in 2021⁶ estimated ownership of cryptocurrencies was up to around 2.3 million individuals globally, an increase from around 1.9 million in 2020—with 78% of adults having heard of cryptocurrencies. The total market capitalization of stablecoins has grown from \$2.6 billion at the start of 2019, to \$20 billion in September 2020—with global trading volumes estimated at \$198 billion in April 2021⁷.

⁵ CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 85+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at <http://www.informationpolicycentre.com/>. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

⁶ Financial Conduct Authority [Research Note: Cryptoasset consumer research 2021 | FCA](#)

⁷ TheCityUK Cryptoassets: [Shaping UK regulation for innovation and global leadership](#)

Decentralized Finance (“DeFi”), a branch of the crypto ecosystem, accounts for a total value locked (“TVL”) in DeFi services from \$600 million in January 1st 2020 to a peak around \$315 billion in December 2021, yielding a growth of 524% in two years⁸. While the TVL has since dropped, it remains well above \$250 billion. In a geographical analysis of DeFi activity, Chainalysis highlights⁹ that a large part of the DeFi growth has been driven by professional and institutional investors particularly from the European financial service sector. It is clear that the economic impact is too significant to be overlooked.

Digital assets in blockchain should be a key priority for the ICO and FCA in 2023 and 2024, and will be of interest to the CMA and Ofcom, as data and digital are core to digital assets. Clear analysis and direction of the interplay of privacy with digital assets will help ensure that the UK is a thought leader in this space, and to establish practical and proportionate approaches which support responsible innovation.

Privacy enhancing technologies

Both in the context of digital assets and more broadly, Privacy enhancing technologies (PETs) can be a useful instrument to safeguard data security as well as data privacy and to bridge tensions with existing data protection frameworks. For instance, zero-knowledge proof technology can verify the authenticity of a given transaction without providing access to the underlying data and has the potential to function as a standard encryption baseline for blockchain applications. PETs have the potential to be deployed broadly and by a larger group of private and public organisations, to mitigate privacy risks, aid and streamline legal compliance and establish trust in the development and use of digital technology. PET research beyond the initial ICO draft guidance should be a further priority on the DRCF work plan, especially in the areas where the different DRCF regulatory disciplines interact and overlap with data privacy rules (e.g. online safety / content moderation and data privacy, data security and data privacy, competition and data privacy, children’s rights and data privacy).

Accountability frameworks

Accountability has become a foundational stone of data privacy law, policy and best practice compliance among both private and public sector organisations. With increased regulatory expectations and the need to establish trusted and responsible data use and, many organisations have been developing privacy management programs to operationalise legal requirements, manage privacy risks and compliance and be able to demonstrate compliance and responsible use of data internally to management, to corporate boards and externally to regulators, auditors, corporate clients. CIPL has done extensive research on accountability and has [published a number of influential papers](#) on the topic.

⁸ European Commission [Decentralized Finance. Information frictions and public policies: approaching the regulation and supervision of decentralized finance](#)

⁹ Chainalysis [The 2021 geography of cryptocurrency report: analysis of geographic trends in cryptocurrency adoption, usage and regulation](#)

The ICO has also emphasised the importance of accountability and has developed their Accountability Framework, to help organisations implement and measure accountability

CIPL very much supports these initiatives. In the context of the DRCF workplan and further priorities, CIPL would like to suggest the following focus areas:

- a) a wider and more explicit recognition by all DRCF regulators of the importance of accountability in their respective regulatory competence;
- b) the development of a consensus and common cross-regulatory framework on the elements of accountability, which are risk-based, outcome based and common to all regulatory areas. CIPL works shows that accountability is law agnostic and can be applied in any area of digital regulation¹⁰. It would be desirable for companies operating in the UK to be able to work with a common framework that can leveraged across all relevant areas of digital compliance with the competence of DRCF regulators;
- c) more proactively incentivising and encouraging by providing tangible benefits for organisations that can demonstrate their digital responsibility in the given regulatory area¹¹.

Cross-regulatory sandboxes

CIPL has been supporting the development and wider adoption of regulatory sandboxes, as developed by the FCA, ICO and CMA. We would like to see further cross-regulatory sandbox projects launched within DRCF, especially in areas with interdisciplinary overlap and interaction – such as online safety/ content moderation and data privacy, or children’s rights and data privacy, of digital assets and data privacy, or competition and data privacy. DRCF should consider proactively putting further resources into the development of such crossregulatory sandboxes. More organisations should be incentivised to participate.

Transborder data flows

Transborder data flows are one of the key areas and yet also the most complex issues of corporate compliance for both large and small organisations. Beyond just regulating the sharing of personal data through data protection laws, we see an increasing trend of data localisation requirements globally. Yet, it is essential to enable free and trusted data flows for the development and deployment of new technologies such as AI, for productivity and efficiency, to enable health and medical research and many other beneficial uses of data, that fuel economic growth and societal progress at large. The UK Government has taken steps to prioritised free, trusted and accountable data flows and has set up an Expert Council to advise on the matter.

¹⁰ CIPL White Paper - [Organizational Accountability - Existence in US Regulatory Compliance and its Relevance for a US Federal Privacy Law](#) and CIPL White Paper - [Organizational Accountability - Past, Present and Future](#)

¹¹ CIPL White Paper - [Organizational Accountability in Data Protection Enforcement - How Regulators Consider Accountability in their Enforcement Decisions](#)

Given that cross-border data flows are inevitable and often essential to all the regulatory domains of the DRCF, CIPL would like to suggest a cross-disciplinary project and working group to identify essential and necessary data flows in the respective areas and consider how these data flows can be enabled in compliance with the existing and, perhaps future new, rules and transfer mechanisms.

ii. In line with the ‘factors we consider when prioritising work’ (see above), are there any areas of focus you believe align with these that are not covered in our previous workplan?

Coherence, Collaboration and Capability themes are all relevant to the intersection of digital assets and privacy. Given the unprecedented growth in this sector, and the need for both innovators and traditional financial institutions to have clarity as to how they can engage in digital assets, it is essential that privacy and financial services partner effectively in regulatory and policy development. In the fight against financial crime, we can see how the balance between requirements to know customers better and monitor financial transactions can create tensions with privacy obligations to limit data processing, particularly of special category and criminal data, and concerns about automated decision making. The UK was able to navigate these tensions through the provisions of the Data Protection Act 2018 (Schedule 1 Section 12), but they remain open issues in many other jurisdictions, leading to uncertainty and an overly cautious approaches to data processing, with the consequences that less than 1% of laundered money is ever recovered¹².

As the nature of digital assets continues to grow and evolve, it is increasingly important that a coherent regulatory approach is developed. Already the Data Protection Authorities in France and Singapore, and the European Parliament and EU (e.g. Markets in crypto-assets Regulation "MiCA") are developing approaches to digital assets, some of which are helpful. If the UK wishes to support a pro-innovation economy, it also needs to be ready to tackle and provide practical policy thought leadership for digital assets on blockchain. Digital Assets are a current reality, not just a future potential, making this an urgent priority for 2023.

iii. Are there any particular stakeholder groups (e.g. end users such as vulnerable consumers, children, businesses) that you believe the DRCF should be particularly mindful of when prioritising areas of focus for the DRCF?

Digital assets have the potential to impact all members of the public, whether through NFT's, crypto currencies, tokenisation of assets, etc. Consumers, businesses and the financial services sector itself are all impacted. A focus on vulnerable consumers and children, as digital assets are made more readily available through social media channels, is certainly a priority. The cross-border nature of digital assets also needs to be addressed.

¹² Forbes [Why Organized Illicit Finance Demands An Organized Global Response](#)

The DRCF is encouraged to be open and consultative going forward to leverage the full breadth of business engagement and to build trust in the model.

An important element of capacity building in stakeholder engagement is the ability to rely on tools that can provide practical support for innovators and greater coherence to the regulators' work. In this sense: the development and adoption of standards and codes of conduct can ease navigation of overlapping regulations; and the simplification of the sandbox model would help decrease the necessary investment and allow start-ups and SMEs to cooperate on potentially less complex issues.

II. Conclusion

CIPL is grateful for the opportunity to provide input to the DRCF workplan 2023/2024. CIPL supports DRCF's work: cooperation between regulators and business takes time and persistence, but we strongly believe it will lead to sustainable outcomes for the digital ecosystem in support of innovation.

If you would like to discuss any of the comments in this paper or require additional information, please contact [REDACTED], [REDACTED], or [REDACTED].

5. Chainalysis

Foreword

Thank you for the opportunity to submit evidence to this DRCF call for input. We are prepared to assist the inquiry using our industry and technical experience to provide further insight should it be considered helpful.

Chainalysis fundamentally believes in the potential of the DRCF as not only a means for cooperation between public bodies but as a means for industry to inform the approach to digital regulation in this space. This will ensure that any regulatory approach is more likely to be sustainable because it has been developed in concert with those it applies to.

About Chainalysis

Chainalysis is a blockchain data and analytics company with over 850 public and private sector customers in over 70 countries. We are a partner to regulators implementing and enforcing anti-money laundering (AML) and countering the financing of terrorism (CFT) and other public policy goals involving digital assets. We are also a partner to law enforcement and other government agencies, which use our products to investigate criminal activity involving digital assets. Businesses also use our products for transaction monitoring and meeting compliance requirements under the UK Money Laundering Regulation (MLRs) and other AML/CFT and related requirements.

Chainalysis's partnerships with law enforcement and regulators are consistent with our mission: to build trust in blockchains. Fundamentally, we believe in the potential of open, decentralised blockchain networks to drive efficiencies, reduce barriers for innovators to create new financial and commercial products, encourage innovation, enhance financial inclusion, and unlock competitive forces across financial services and other markets.

Our tools have been used in several successful digital asset investigations, including, but not limited to, the [Mt. Gox](#) hack, North Korean [crypto hacking cases](#), the [Colonial Pipeline attack](#), and the OFAC designation of [Suex](#), a digital asset exchange that facilitated money laundering for a number of illicit actors, including ransomware gangs. More recently, Chainalysis assisted law enforcement partners in an investigation following the March 2022 DPRK theft of more than \$600 million from Ronin Network. This investigation led to the seizure of more than \$30 million worth of cryptocurrency stolen by North Korean-linked hackers and marks the most significant seizure of cryptocurrency stolen by a North Korean hacking group.

Question 3: *Are there any particular stakeholder groups (e.g. end users such as vulnerable consumers, children, and businesses) that you believe the DRCF should be particularly mindful of when prioritising areas of focus for the DRCF?*

Public-Private partnerships as a crucial part of the approach to digital assets

The importance of knowledge sharing between regulators is central to the DRCF, and for a good reason. However, a significant amount of expertise, insight, and data sits outside the public sector and this particular forum that could have a considerable impact if it were utilised effectively.

Take, for instance, the approach to building engagement between Ofcom and the FCA on online fraud and scams. Missing from this picture is an acknowledgement that industry can greatly assist when it comes to understanding the threat landscape. Not only can this be of use during the policymaking stage with the design of suitable approaches and frameworks, but also in the implementation stage where supervisory action and monitoring are required.

Understanding the landscape and the tools available in the new digital ecosystem by partnering with the public sector can only be additive to both processes and allow for a more nuanced understanding and more effective response. There is currently no effective forum for this kind of public-private partnership in the UK regarding digital assets. It may be worth considering the example of the U.S. Department of Treasury's Financial Crimes Enforcement Network ("FinCEN") Exchange program, which brings together representatives from FinCEN, law enforcement, regulators, and industry members in a voluntary public-private information-sharing partnership.

These exchanges enable FinCEN to collect and share information in a less formal setting and learn about the industry's challenges in preventing illicit finance. These sorts of public-private partnerships help to build and improve relationships and sharing mechanisms across the public-private divide, with the goal of preventing illicit finance and protecting end consumers.

Others recognise the importance of increasing public-private cooperation as it regards financial crime. Take, for example, the Recommendations of the Joint Working Group on Criminal Finances and Cryptocurrencies from the Europol and the Basel Institute on Governance. Their report recognises that closer cooperation with industry can have significant positive effects on addressing instances of digital asset-related crime by understanding and deploying the range of private sector tools and depth of insight that exists.¹³

Beyond the utility of public-private partnerships for tackling financial crime in digital assets, there is value in encouraging such partnerships for other use cases and regulatory approaches to digital. Structuring around focus areas and technology themes can ensure that all relevant

¹³ Seizing the opportunity: 5 Recommendation for cryptoassets-related crime and money laundering - 2022 Recommendations of the Joint Working Group on Criminal Finances and Cryptocurrencies"

https://www.europol.europa.eu/cms/sites/default/files/documents/2022_Recommendations_Joint_Working_Group_on_Criminal_Finances_and_Cryptocurrencies_.pdf



agencies and private sector actors are brought to the table and that the forum becomes a more effective medium for collaboration and information sharing.

6. Coventry University

Please may I suggest that research institutes/universities working in the area of the four UK regulators (CMA, Ofcom, ICO and the FCA) be included in ‘**Collaboration on projects**’. The call states:

“... there is significant benefit in us coming together to address complex problems in areas of common interest. While we each need to deal with issues and make decisions in a bespoke way to deliver on our regulatory duties, we have opportunities to work together to achieve common goals. Doing this will allow us to work more efficiently, avoid duplicated efforts, develop shared approaches and deliver joint guidance for industry where appropriate.”

Coventry University lead an **EU funded** international project, [CSI-COP](#), investigating GDPR compliance specifically in websites and apps with respect to transparency about, and informed consent for, third-party tracking: <https://cordis.europa.eu/project/id/873169>

The **CSI-COP** project won an industry award for ‘**Best Innovative Privacy Project**’ in the inaugural [PICCASO privacy awards](#) in December 2022: <https://www.picasoprivacyawards.com/blog/piccaso-privacy-awards-winners-announced-celebrating-the-brightest-and-best>

CSI-COP leverages a **citizen science methodology** raising awareness amongst the general public about the extent of online tracking. and also increasing the scientific literacy of citizens by providing a free informal education resource ‘**Your Right to Privacy Online**’ in English and twelve translations: <https://csi-cop.eu/informal-education-mooc/>

The impact of CSI-COP is evident from the project’s **privacy-by-design, no-tracking website** influencing Coventry University’s own website to be more transparent and clearer about its cookie notices. CSI-COP partners have also worked towards changing their organisational websites to be more GDPR-compliant. [CSI-COP’s first policy brief](#) recommended that at least EU funded projects should create privacy-by-design websites. Further recommendations will include putting forward standards for cookie banners and privacy policies to make these more transparent and easier to understand.

Coventry University contributing to the DRCF as the co-ordinating body could further bring together a variety of stakeholders. The purpose would be to benefit individuals and all kinds of businesses online increasing trust between stakeholders, and promoting the development of more trustworthy digital artefacts/ tools that protect data and privacy online, especially children’s data and privacy, since they also have human rights.

I very much look forward to collaborating with the DRCF wherever possible in the future. Thank you for your time.

Sincerely,
Huma

--

Dr. Huma Shah

-Director of Science (Co-PI), EU Horizon2020 **CSI-COP** research and innovation
project: <https://csi-cop.eu/>