JOINT POSITION STATEMENT
PREVENTING FRAUD ON SOCIAL MEDIA

FRAUDSTERS ARE IMMERSED IN SOCIAL MEDIA JUST LIKE THE REST OF US. THEY USE IT EXTENSIVELY TO PLAN AND COMMIT CRIME BECAUSE IT IS FAST, CONVENIENT AND LOW-RISK.

It lets them locate, research and groom their victims with near impunity, hidden behind a veil of anonymity. They can also contact, recruit, network and conspire with other criminals openly, without fear of reprisals.

Because we need to stop criminals from misusing social media to commit fraud and cybercrime, we are calling for a complete re-think of our online defences.

Current remedies, including the Online Safety Bill, must be broad-based and future proofed (as best we can); focused on the harms done not just the technology used to deliver them.

Social media providers should also know all their customers and make their online platforms safe for users (just like other businesses).

THE PROBLEM

- Online friendship and talk of romance help criminals defraud the lonely and lovelorn.
- Fraudsters amplify their crimes by first tricking or bribing 'social media influencers' into getting the word out.
- 'Dognappers' target victims by analysing owners' social media posts.
- Adverts for non-existent jobs harvest personal information and demand money.
- Money mules are recruited via social media posts offering cash.
- Plausible online adverts reel in the victims of investment fraud.
- Customers are conned by criminals impersonating genuine businesses.
- Thefts of customer data or business information begin with the targeted grooming of staff on social media.

The list goes on and on.

Researchers say it makes more sense to list the very few fraud types that don't make use of social media, rather than the vast majority that do.

And yet policing of online fraud and cybercrime remains under-prioritised and underfunded, just as it always has been. There are so few successful investigations and prosecutions that criminal justice outcomes are barely any deterrent, even though they could be.

ONE IN FIFTEEN PEOPLE IS A VICTIM OF FRAUD EACH YEAR IN THE UK, WITH THE INTERNET BELIEVED TO PLAY A ROLE IN MORE THAN HALF.

COMPUTER MISUSE OFFENCES WERE UP LAST YEAR BY 36% TO 1.7M – MOSTLY DRIVEN BY HACKING OF SOCIAL MEDIA AND EMAIL.

FRAUD AGAINST INDIVIDUALS COSTS AT LEAST £4.7BN ANNUALLY; FOR BUSINESSES AND THE PUBLIC SECTOR IT'S £5.9BN.

SOCIAL MEDIA FEATURED IN AT LEAST 61,000 CRIME REPORTS TO ACTION FRAUD IN 2020-21, WITH LOSSES OF MORE THAN £120M.

AUTHORISED PUSH PAYMENT FRAUD LOSSES TOTAL £479M EACH YEAR WITH MANY VICTIMS MANIPULATED ON ONLINE PLATFORMS INCLUDING SOCIAL MEDIA.

A NEW SCAM AD ALERT SYSTEM RECEIVED 1,274 REPORTS OF ONLINE SCAM ADS IN ITS FIRST SIX MONTHS.

ACTION NOW

1. INCLUDE FRAUD AND CYBERCRIME (AS WELL AS THE HARMS DONE TO BUSINESSES) IN THE FORTHCOMING ONLINE SAFETY BILL

Much financial, emotional and psychological harm is indivisible. Lying and bullying online often have an economic motive. Psychological and emotional pain is frequently a long-lasting consequence of fraud. Meanwhile, 96% of UK businesses have fewer than ten employees and are often 'vulnerable' in their own way.

2. CREATE A VOLUNTARY FRAUD CHARTER FOR SOCIAL MEDIA PROVIDERS

Set out their duty of care to users. Ideally this should include: on-screen warnings; reporting mechanisms for all fraudulent, misleading and harmful material; standards for timely removal of suspect material; and a means for users to seek redress.

3. ENCOURAGE VOLUNTARY ADOPTION OF VERIFIED IDS

Users should be able to have confidence in businesses that have undergone enhanced due diligence checks. In the longer-term, consider verified IDs for all users.

ACTION IN THE LONGER TERM

4. REVIEW THE DOMESTIC LEGAL FRAMEWORK WITH RESPECT TO ONLINE FRAUD AND CYBERCRIME

Pay particular attention to the Computer Misuse Act, now wildly out-of-date and completely unfit for the times.

5. LAUNCH A PUBLIC AWARENESS CAMPAIGN

This should be well-funded and sustained – and evaluated carefully – to help users think more critically about what they see and experience online. Facebook has already done this for COVID-19 vaccine misinformation. We see no reason why it can't be replicated for other forms of online abuse and deception, and by other social media providers.

REFERENCES

Action Fraud and National Fraud Intelligence Bureau. (2021) *Social media statistics request.* City of London Police, 9 April.

Advertising Standards Association. (2021) *Six month review of our Scam Ad Alert System.* Press release, 02 March.

Business Wire. (2019) *More Than Half of Logins on Social Media Platforms Are Fraud, as Arkose Labs Report Exposes Targeted Industries and Unique Attack Patterns.* Article, 26 August.

Department for Business, Energy & Industrial Strategy. (2020) *National Statistics: Business population estimates for the UK and regions 2020: statistical release.*

Facebook. (2021) *Reaching Billions of People With COVID-19 Vaccine Information.* Press release, 8 February.

Fell, E., James, O., Dienes, H., Shah, N., and Grimshaw, J. (2019) *Understanding organised crime 2015/16: Estimating the scale and the social and economic costs: Second edition.* Home Office. Research Report 103.

Fletcher, E. (2020) *Scams starting on social media proliferate in early 2020.* Federal Trade Commission. Blog, 21 October.

Heeks, M., Reed, S., Tafsiri, M., and Prince, S. (2018) *The economic and social costs of crime: Second edition.* Home Office. Research Report 99.

HM Government and UK Finance. (July 2019) *Economic Crime Plan 2019-22.*

House of Commons Treasury Committee. (25 January 2021) *Oral Evidence: Economic Crime,* HC 917.

National Crime Agency. (2020) *National Strategic Assessment of Serious and Organised Crime 2020.*

Office for National Statistics. (2021) *Crime in England and Wales: year ending September 2020.*

UK Finance. (2021) *Fraud – The Facts 2021.*

Wood, H., Keatinge, T., Ditcham, K., and Janjeva, A. (2021) *The Silent Threat: The Impact of Fraud on UK National Security.* RUSI. Occasional Paper.

WE STAND READY TO SUPPORT COLLECTIVE EFFORTS TO STOP FRAUD ON SOCIAL MEDIA. IN A FAST-CHANGING WORLD WE CAN FIGHT FRAUD BY WORKING TOGETHER.

FRAUD ADVISORY PANEL

CARDIFF UNIVERSITY
PRIFYSGOL CAERDYDD

cifas
Leaders in fraud prevention

CDA

PREVENTION OF FRAUD IN TRADE LTD

GUILDHAWK
TRUSTED IN ANY LANGUAGE

MOON BEEVER
SOLICITORS

SYNECTICS SOLUTIONS

tenet
compliance & litigation

Telecommunications UK Fraud Forum
TUFF