

THE RISE OF FINANCIAL DISINFORMATION

A CCOD report on market manipulation in the digital age

CCOD

The Rise of Financial Disinformation

Market Manipulation in the Digital Age

Content

Executive summary 1

1. **The Threat: What is financial disinformation?** 2

2. Why it's getting worse 3

3. The Impact of Financial Disinformation 6

3.1 Impact on businesses and share prices 6

3.2 Impact on financial stability: Social-media bank runs 7

3.3 Macro-level market manipulation 9

3.4 Impact on individuals and consumer behaviour 11

4. Recommendations 12

5. Conclusion 14

Executive summary

The World Economic Forum ranks disinformation as the top global risk for 2025. Edelman found that 8 in 10 executives are concerned about AI-driven disinformation. Nearly 80% admitted their businesses were not adequately prepared.



[1]

This report by the Council on Countering Online Disinformation (CCOD) examines the nature of financial disinformation – false information that is deliberately spread with malicious intent and financial motive. The report analyses its real-world impact through case studies, and showcases policy recommendations for businesses and regulators.

Our analysis identifies that a whole range of actors and industries are already at threat through financial disinformation: corporations, individuals, the economy and society. The threat is growing in scale and increasing in sophistication due to AI. The Silicon Valley Bank collapse of 2023 demonstrated that social media-amplified panic can destroy a $209 billion institution in under 48 hours. The Arup deepfake fraud showed that a single AI-generated video call can yield $25 million in criminal proceeds. These and other real-world cases show that it is high time to prepare policy interventions to meet this threat.

To counter disinformation, the CCOD believes any effective strategy should not lie in waiting but tackle the problem from different angles and throughout time. The CCOD believes the best approach is rooted in **leveraging innovation in the short-term, pragmatic and nimble regulatory interventions in the medium term, and media literacy and awareness in the long term**. Ultimately, the **financial incentives for spreading false content need to be removed** from platforms by demonetising misinformation and holding both platforms and advertisers accountable. With coordinated action across the private sector, government and civil society, its worst effects can be anticipated, mitigated and increasingly reversed.

[1] 1: Sopra Steria. (2026, March 12). *Disinformation's global economic impact estimated at $417 billion in Sopra Steria study*. *2:* Serrano, J. (2025, July 14). *What's the real cost of disinformation for corporations?*. World Economic Forum. 3: Edelman. (2024). *2024 Connected Crisis Study – Edelman Crisis & Risk Report*.

1. The Threat: What is financial disinformation?

Financial disinformation is not a new problem. History is rife with examples of deliberate spreading of false or misleading content for economic gain. What is new is the way AI and social media platforms are altering the threat both in scope and in kind.

The World Economic Forum now ranks **disinformation as one of the top global risks** for 2025.[2] Last year, an Edelman Crisis and Risk report found that 8 in 10 executives are concerned about the negative impact **AI-driven disinformation** can have on their business, and almost 80% admit that their businesses are not adequately equipped to face these threats.[3] But what is disinformation?

The Council of Countering Online Disinformation (CCOD) defines **disinformation** as **false information that is deliberately spread with malicious intent.** This distinguishes it from misinformation, which is spread *without* malicious intent (as a genuine mistake). **Based on the type of intent**, the CCOD defines three main types of online disinformation: **financial, ideological, and disruptive disinformation** without a clear ideological or financial aim.

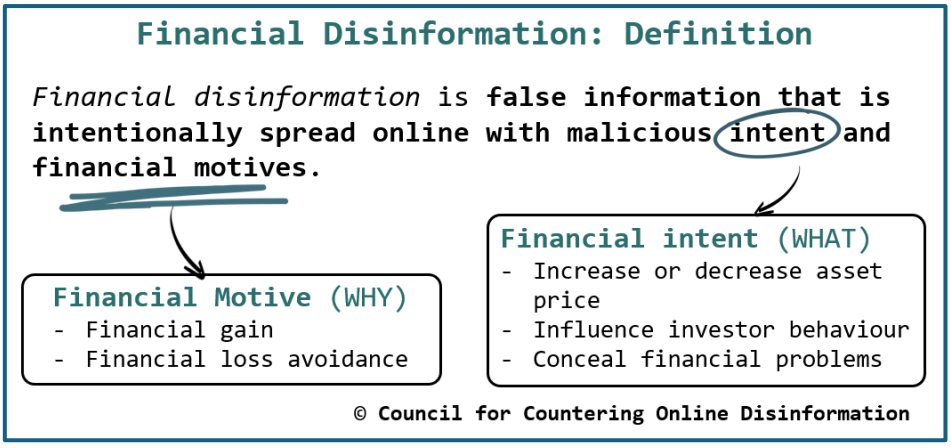
Types of Online Disinformation

	Intent	Manifests as…
Financial Disinformation	**Economic/Financial,** e.g. financial gain or loss avoidance	Stock market, corporate valuation or consumer product perception manipulation
Ideological Disinformation	**Political/ideological,** e.g. increasing or decreasing political or ideological support, influencing political outcomes	Election interference, (policy) debate manipulation, public opinion manipulation
Disruptive Disinformation	**Personal** *(without advancing coherent ideological or financial goal)*, e.g. revenge, attention, creating chaos	Trolling, rage-baiting, online defamation or false claims for attention and social media engagement

© Council for Countering Online Disinformation

Financial disinformation is a specific sub-type of disinformation which has **financial motives and intents**.

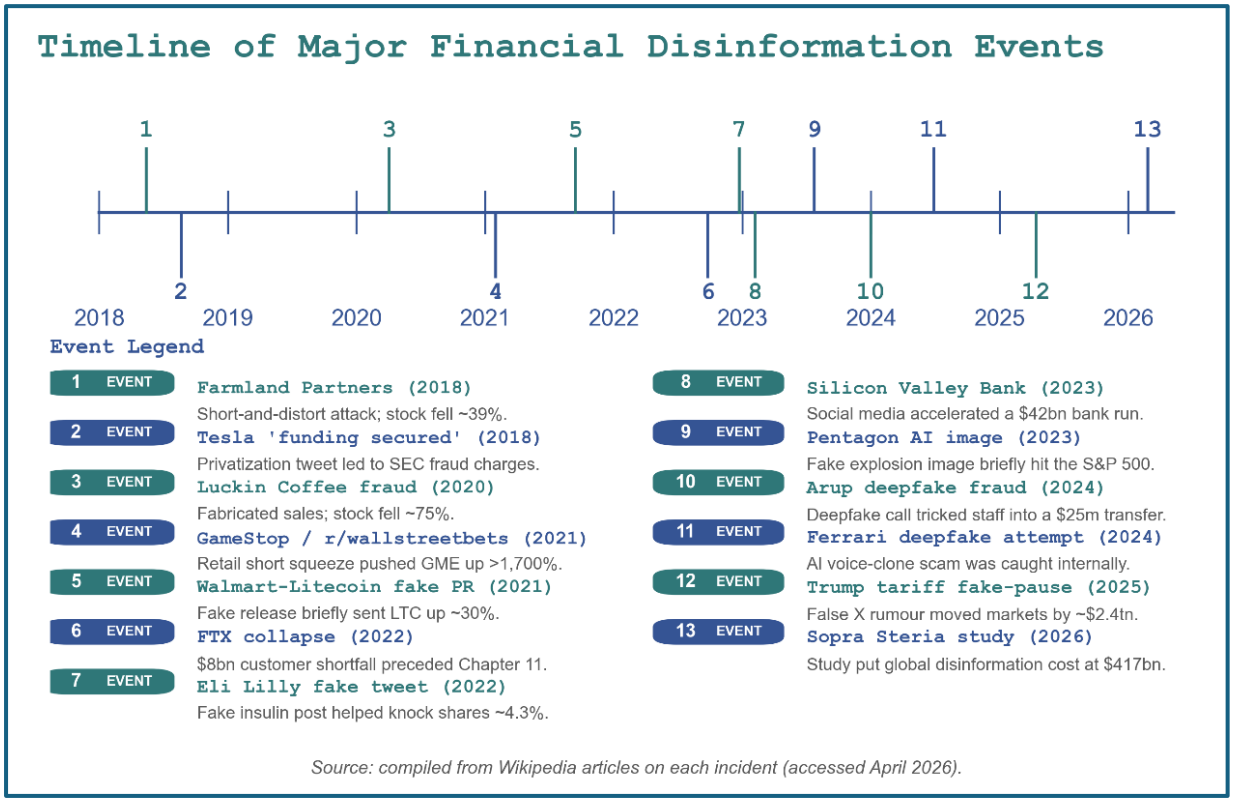
[2] World Economic Forum. (2025). *Global Risks Report 2025*.
[3] Edelman. (2024). *2024 Connected Crisis Study – Edelman Crisis & Risk Report*.



Different **methods** are used to create and spread financial disinformation, including AI-generated deepfakes, voice impersonation, cyber-phishing, reputational attacks, fake reviews or fake posts on social media.

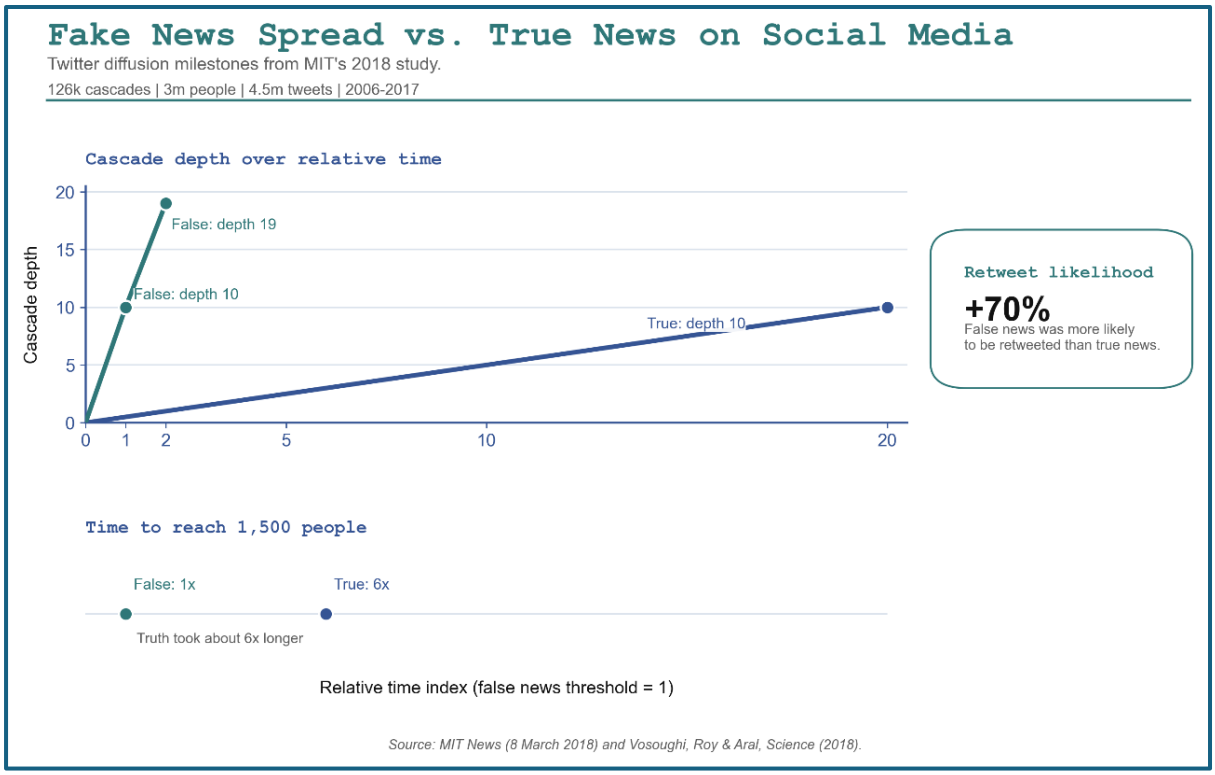
2. Why it's getting worse

With the financial world increasingly operating online, there are significant risks for companies that need to navigate disinformation threats in real time. The sheer speed at which disinformation can spread is such that share prices, the reputation of a company's product, or the credibility of a banking system can be affected – and often upended – in hours.



Research published in 2018 by MIT found that **false news stories are 70% more likely to be retweeted than true ones**, and that **false information reaches the same number of**

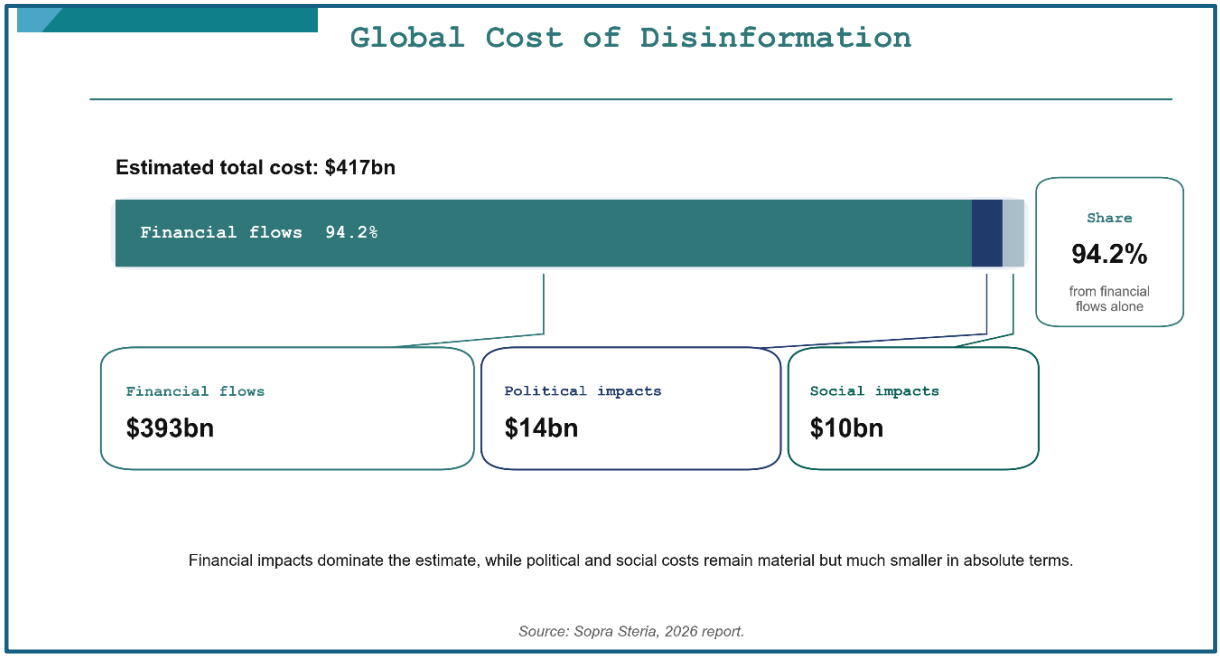
people six times faster than true information. This is in part because disinformation tends to be more emotionally charged or novel, which are qualities that drive online engagement.[4] With **AI making the creation of false or misleading content easier and faster**, these statistics are likely to have worsened since the study came out in 2018. This algorithmic amplification, combined with the ease of mobile banking and instant transfer possibilities, has created conditions in which the consequences of disinformation can be felt almost instantaneously.



Generative AI has dramatically lowered the cost and raised the quality of disinformation production. Deepfakes that once required specialist skills can now be created very cheaply in minutes. The level of realism and constantly changing technological capabilities make detection very difficult.[5] A study on deepfakes of Dutch and American politicians showed that even deepfakes which were assessed as implausible by test subjects (deepfakes with political statements far removed from the ideology of the politician) were, notwithstanding, still very effective at delegitimising the politician in the public eye, even more so than deepfakes manipulated more credibly.[6] Disinformation becomes particularly effective and dangerous when synthetic content is microtargeted and its message can be tailored to specific audiences.

[4] MIT News Office (2018, March 8). *Study: On Twitter, false news travels faster than true stories*.
[5] Campante, F., Durante, R., Hagemeister, F. & Sen, A. (2025). *AI misinformation and the value of trusted news*. Centre for Economic Policy Research (VoxEU).
[6] Hameleers, M., Van der Meer, T. G., & Dobber, T. (2024). Distorting the truth versus blatant lies: The effects of different degrees of deception in domestic and foreign political deepfakes. *Computers in Human Behavior*, *152*, 108096. https://doi.org/10.1016/j.chb.2023.108096.

At the same time, disinformation has become a business, and targeted disinformation campaigns against actors or institutions can be purchased, which means that both **individuals as well as state-sponsored actors can execute attacks at scale**. Researchers at the Oxford Internet Institute have discovered that in more than a third of the 70 countries evaluated, state actors had commissioned disinformation-for-hire companies with computational propaganda.[7] Disinformation experts see realistic AI-generated videos as particularly effective in creating strong emotional reactions, but see large-scale text generation as the graver long-term threat due to its potential to create a "synthetic consensus" and break down established and evidence-based understanding of issues and facts.[8]

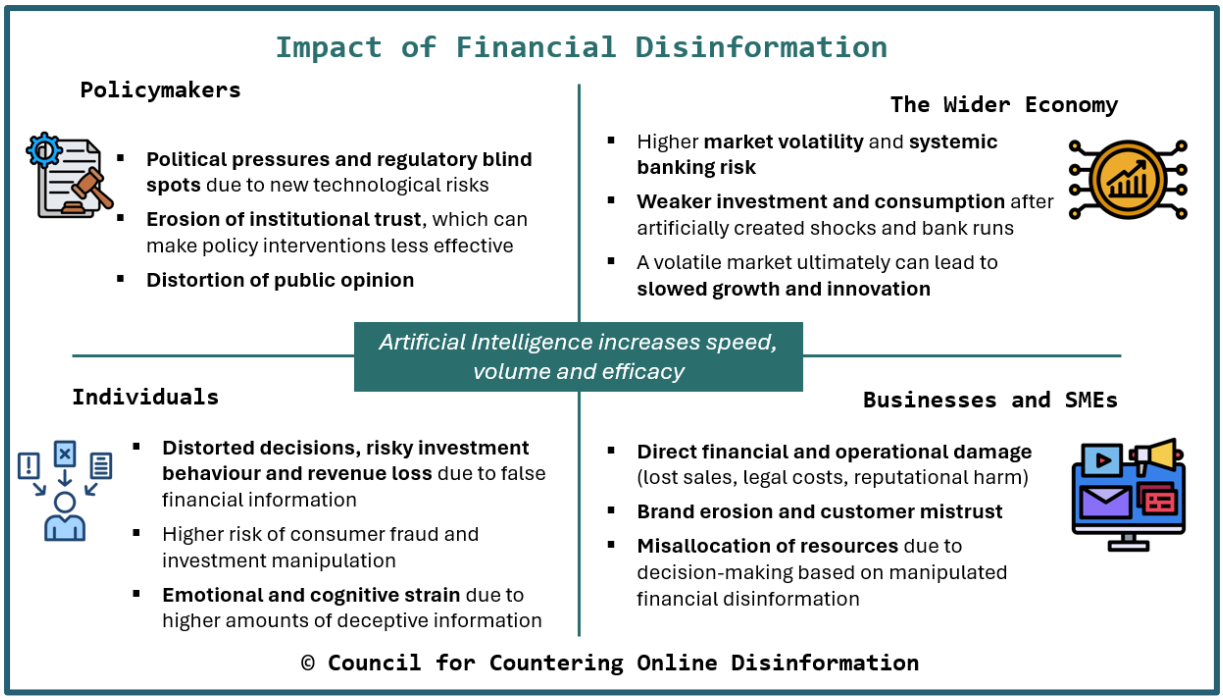


Keeping up with these changes requires upskilling the digital literacy of citizens and businesses but also putting in place nimble, effective regulation. A number of case studies will be reviewed in following sections of this report to identify pragmatic policy recommendations. As we are dealing with an evolving threat, financial disinformation may change guise or its level of penetration, but the CCOD seeks to identify and put forward certain aspects of best practice that can remain constant and at the ready in the toolboxes of businesses and policy makers.

[7] Bradshaw, S., & Howard, P. N. (2019). *The Global Disinformation Disorder: 2019 Global Inventory of Organised Social Media Manipulation* (Working Paper 2019.2). Oxford, UK: Project on Computational Propaganda.
[8] Loth, A., Kappes, M., & Pahl, M.-O. (2026). *The Verification Crisis: Expert Perceptions of GenAI Disinformation and the Case for Reproducible Provenance*. *Companion Proceedings of the ACM Web Conference 2026 (WWW Companion '26)*. https://doi.org/10.48550/arXiv.2602.02100.

3. The Impact of Financial Disinformation

To understand the full harm potential of financial disinformation, this section will break down the risk by its impact on different stakeholders and industries, and include a prominent example for each: individual businesses, financial stability and market manipulation at systemic level, and individual consumers.



A 2024 study by Sopra Steria calculated, for the first time to date, the **estimated global impact of disinformation: $417 billion**. This is broken down into the three impact categories financial flows ($393 billion), political impacts ($14 billion) and social impacts ($10 billion).[9] This estimate is far higher than the $78 billion figure estimated in 2019 by CHEQ and the University of Baltimore.[10] The increase reflects that the threat has intensified: due to the rise of AI, wider use of disinformation in geopolitical conflicts, and slow, often ineffective responses from Western democracies.

3.1 Impact on businesses and share prices

In 2022, the stock price of the pharmaceutical company Eli Lilly dropped 4.37% after a fake company account had tweeted that insulin would be made available for free.[11] This and other cases shows that for publicly listed companies, financial disinformation poses a large threat to market value. Recent research by Liu and Moss found **that fake financial news has been rising steadily** since 2016. Companies with less transparent financial

[9] Sopra Steria. (2026, March 12). *Disinformation's global economic impact estimated at $417 billion in Sopra Steria study*.
[10] CHEQ & University of Baltimore. (2019). *The Economic Cost of Bad Actors on the Internet: Fake News*.
[11] Lee, B. Y. (2022, November 12). *Fake Eli Lilly Twitter account claims insulin is free, stock falls 4.37%*. Forbes.

reporting were the most at risk because disinformation actors most frequently target firms whose financials are harder to scrutinise.[12]

A 2023 study by Arcuri et al. looked at information-based manipulation of financial markets. Their research revealed that negative **fake news had a negative impact on market returns** in the short term, thereby establishing a direct link between negative disinformation and adverse market reactions. Interestingly, they found that positive or neutral news items did not have a direct impact on stock returns.[13]

Next to the market loss incurred, the **reputational damage** which follows can add a significant layer of cost through crisis management, legal fees and loss of customer trust, the latter which can be hard to restore once lost. The case study below of Farmland Partners is a good example of deliberate financial disinformation targeting a publicly listed company, and the subsequent reputational burden and long-lasting legal processes that can follow.

CASE STUDY: FARMLAND PARTNERS: THE 'SHORT AND DISTORT' SCHEME (2018)

In July 2018, the anonymous author 'Rota Fortunae' published an article on a financial website with a series of false allegations against Farmland Partners Inc., a Colorado-based real estate investment trust. The article falsely claimed that 310% of the company's last year's earnings were fabricated, accusing the management of fraud and claiming that the company faced insolvency.

The article drove the company's share price down by 39% on the day of publication alone — wiping out more than $115 million of market value. The anonymous author had taken short positions in the company's stock before the article was published, as had his clients, including hedge fund Sabrepoint Capital Management.

After years of litigation, the author admitted the article contained numerous false statements, and agreed to repay a multiple of the trading profits made from the scheme. A federal court subsequently dismissed a related class action against the company, concluding that no jury could reasonably find in the plaintiff's favour.[14]

3.2 Impact on financial stability: Social-media bank runs

Perhaps the most alarming dimension of financial disinformation is its **capacity to destabilise entire financial institutions**. The collapse of Silicon Valley Bank (SVB) in March 2023 (see case study below) is a real-world case which shows how social media-

[12] Liu, B., & Moss, A. (2025). The role of accounting information in an era of fake news. *Journal of Accounting and Economics, 79*(2). https://doi.org/10.1016/j.jacceco.2024.101764.
[13] Arcuri, M. C., Gandolfi, G., & Russo, I. (2023). Does fake news impact stock returns? Evidence from US and EU stock markets. *Journal of Economics and Business, 125–126*, 106130. https://doi.org/10.1016/j.jeconbus.2023.106130.
[14] Farmland Partners Inc. (2021). *'Rota Fortunae,' author of July 2018 attack on Farmland Partners, retracts short and distort article, admits article's falsity, and returns multiples of trading profits he gained from attack*.

amplified panic can trigger a devastating bank run. On 8 March 2023, after an announcement of incurred financial loss, social media disinformation led to customers trying to withdraw $42 billion in a single day. Patrick McHenry, then chairman of the US House Financial Services Committee, described SVB's collapse as 'the first Twitter-fuelled bank run.'[15]

The Federal Deposit Insurance Corporation (FDIC), in a 2024 report, concluded that while social media is unlikely to be the sole cause of a bank run, its capacity to rapidly distribute (false) information across a whole platform represents a **grave risk to banking stability**. They also evaluated that banks with the highest social media exposure lost approximately twice as much stock market value as those with lower exposure. The key mechanism was not negative sentiment per se, but the sheer volume and speed of public conversation, which accelerated the coordination of mass withdrawals.[16]

A simulation exercise conducted by Say No to Disinfo and Fenimore Harper Communications tested whether an AI-powered disinformation campaign could trigger a bank run in the UK. Using readily available AI tools, the team generated false headlines and fake social media posts suggesting customer deposits were at risk. **60.8%** of polled individuals exposed to the campaign expressed a likelihood of moving their money. The researchers estimate that **for every £10 spent on ads**, **as much as £1 million** could be moved.[17] This shows that the same dynamics that brought down SVB could also be used to bring down the UK banking system, at very little cost.

CASE STUDY: THE SVB COLLAPSE: SOCIAL MEDIA AND THE FIRST TWITTER BANK RUN (2023)

Silicon Valley Bank, previously valued at $209 billion and then 16th biggest bank in the US, collapsed on 10 March 2023 after a social media-induced bank-run, making it the largest bank failure in the United States since Washington Mutual in 2008.

SVB had been operating for 40 years, when on 8 March 2023 it announced a $1.8 billion loss from asset sales. The announcement, pitched at regulators and analysts, failed to reassure ordinary customers. In the vacuum of clear communication from the bank, social media filled the void.[18]

While the collapse can also be attributed to poor risk management and rising interest rates, the speed and severity of the bank run which eventually led to the collapse can be attributed to social media. Investor-centric tweets about SVB's stock ticker spiked approximately two and a

[15] Yerushalmy, J. (2023, March 16). 'The first Twitter-fuelled bank run': How social media compounded SVB's collapse. *The Guardian*.
[16] Cookson, J. A., Fox, C., Gil-Bazo, J., Imbet, J. F., & Schiller, C. (2023). Social media as a bank run catalyst. *SSRN*.
[17] Fenimore Harper Communications. (2025). *Can AI Cause a Bank Run?*
[18] Khan, M. H., Hasan, A. B., & Anupam, A. (2024). Social media-based implosion of Silicon Valley Bank and its domino effect on bank stock indices: Evidence from advanced machine and deep learning algorithms. *Social Network Analysis and Mining, 14*, 110. https://doi.org/10.1007/s13278-024-01270-5.

half hours before broader public discussion of the bank began, as depositors coordinated their withdrawals in real time on Twitter, Slack and WhatsApp.

High-profile voices accelerated the panic. Silicon Valley investor Jason Calacanis posted a tweet which was viewed 4.9 million times, reading 'YOU SHOULD BE ABSOLUTELY TERRIFIED RIGHT NOW'. SVB, by contrast, waited over 22 hours before issuing public communications to reassure customers, allowing the panic to compound unchecked.

3.3 Macro-level market manipulation

Financial disinformation can also target markets more broadly to generate **volatility for profit or for the sake of political disruption**. In 2023, an AI-generated image of an explosion near the Pentagon sent shockwaves through stock markets. The S&P 500 dropped 0.3% in response. The fake image began quickly circulating on social media. The Russian government-backed news agency RT quickly posted a tweet: “Reports of an explosion near the Pentagon in Washington DC”; they later took down the tweet after it became apparent that the image was fake.[19]

Research published by the Centre for Economic Policy Research in 2024 found that technology-related fake news **increases economic uncertainty and amplifies business cycle fluctuations**. Policymakers, the authors conclude, cannot afford to treat disinformation as solely a political or social problem: it has direct macroeconomic consequences.[20]

The scale of market manipulation risk is compounded by the accessibility of deepfake tools. Fabricated videos of executives delivering unexpected earnings guidance, or AI-generated images of industrial incidents at major listed companies, require minimal technical skill to produce but can generate immediate and measurable market disruption. Disinformation designed to induce market panic may increasingly serve as a first-order **tool in coordinated campaigns by hostile state actors**. The 2023 Pentagon deepfake incident demonstrated how a single fabricated image could move equity markets within minutes. This attack could be scaled deliberately as part of a hybrid warfare strategy, and such operations could target critical economic infrastructure, shaping distortions during earnings seasons, in the wake of central bank announcements, or in periods of heightened geopolitical tension, all to maximise international social and financial disruption.

A 2025 policy brief by the German Council on Foreign Relations identifies the sabotage of financial market infrastructure as one component of Russia's expanding hybrid threat repertoire, alongside cyber operations, disinformation campaigns, and economic

[19] The Associated Press. (2025, October 28). Pentagon explosion misinformation rattles stock market, highlights AI-driven risk. *AP News*.
[20] Assenza, T.; Collard, F.; Feve, P. & Huber, S. (2024). From buzz and bust: How fake news shapes the business cycle. *VoxEU*.

coercion.[21] The EU Council has similarly recognised this escalation, broadening its sanctions framework in 2025 to target financial backers of Russia's destabilising activities and noting that hybrid campaigns have intensified significantly since the full-scale invasion of Ukraine.[22]

The convergence of accessible generative AI tools and established state-backed influence infrastructure creates a compounding risk. The EUvsDisinfo project documented the emergence of a full-scale disinformation-for-hire industry in 2025, with influence operations increasingly outsourced, professionalised, and augmented by artificial intelligence.[23] Where financial disinformation was once the province of individual bad actors seeking short-term trading profits, the prospect of state-level coordination, which combines synthetic media, bot networks, and proxy news outlets, shifts market manipulation from a mere securities regulation enforcement problem into a **matter of national economic security**.

CASE STUDY: THE ARUP DEEPFAKE FRAUD (2024)

In 2024, the Financial Times reported that British engineering group Arup became the victim of one of the largest deepfake-enabled financial frauds ever recorded. An employee of the company was deceived into authorising fifteen transfers totalling $25 million after participating in a video conference call in which all other participants, including the apparent CFO, were AI-generated deepfakes. The Hong Kong police confirmed this as one of the world's biggest financial scams.[24]

Where earlier corporate fraud required either access to internal systems or the physical impersonation of individuals, generative AI now enables criminals to fabricate entirely convincing video conference calls involving multiple identities simultaneously. The International Compliance Association notes that no single countermeasure is sufficient: protection requires multiple overlapping layers of defence, including AI detection tools, multi-factor authentication and dual-authorisation policies for significant financial transactions.[25]

In 2024 alone, it is estimated that half of all businesses globally were victims of some form of deepfake attack, with average losses per incident estimated at $450,000.[26] The Arup fraud exceeds this average by more than 50 times.

[21] Baumann, M. & Pynnöniemi, K. (2025). European Security in the Era of Hybrid Warfare (DGAP Policy Brief No. 20). German Council on Foreign Relations.
[22] Council of the European Union. (2025). Russian Hybrid Threats: Council Sanctions Twelve Individuals and Two Entities over Information Manipulation and Cyber Attacks. December 15 Press Release.
[23] EUvsDisinfo. (2025). 2025 in Review: Winning the Narrative. European External Action Service (EEAS)
[24] Leng, Ch. & Ho-him, Ch. (2025, August 29). *How AI-driven trading is intensifying market instability*. Financial Times.
[25] International Compliance Association. (2025). *Deepfakes: Strengthening Business Resilience Against the Unknown – Part 2: Improving Cyber Policies and Procedures*. ICA Insight.
[26] Serrano, J. (2025, July 14). *What's the real cost of disinformation for corporations?*. World Economic Forum

3.4 Impact on individuals and consumer behaviour

The impact of financial disinformation is not limited to large corporations and financial markets. Consumer fraud losses in the United States rose by 25% year-on-year to exceed $12.5 billion in 2024.[27] Research from the CFP Board's 2025 survey of Americans found widespread exposure to financial misinformation, with many individuals reporting that it influenced their financial decision-making, and **3 in 5 Americans regretting a financial decision that they had made on the basis of financial misinformation**.[28]

One of the main trends in AI-generated scams that thrives on misinformation are **"pump and dump" schemes**. These are a type of scam with two phases: in the first phase, scammers will spread and promote false or misleadingly positive investment information (often on cryptocurrencies or certain stocks) that are meant to entice individuals to buy in. They frequently claim that their recommendations are based on advanced AI forecasting models. As more people invest, this artificially inflates the price of the asset — the "pump" phase of the scam. Once the price has risen, the scammers sell their holdings at a profit (the "dump"), which can cause the price to fall again and leave other investors with losses.[29]

A study of Indonesian social media users in 2025 found that 37.4% of surveyed investors had been exposed to economic conspiracy theories, and 22.6% admitted that these narratives influenced their investment decisions.[30] While no similar numbers are available for the UK, online influencers and algorithmic amplification are likely to have a similar effect.

[27] Federal Trade Commission. (2025, March). *New FTC data show big jump in reported losses to fraud to $12.5 billion in 2024*.
[28] CFP Board. (2025). *Steering clear of financial misinformation: A 2025 survey of Americans*. CFP Board of Standards.
[29] Financial Conduct Authority. (2025). *Pump and dump schemes*.
[30] Sonni, A. F. (2025). Digital disinformation and financial decision-making: Understanding the spread of economic conspiracy theories in Indonesia. *Frontiers in Human Dynamics, 7*, 1617919. https://doi.org/10.3389/fhumd.2025.1617919.

4. Recommendations

We believe a mix of both reactive and proactive solutions are needed to address the threat of financial disinformation.

Short Term: Detection and Organisational Preparedness. For businesses to protect themselves as soon as possible, they need the right information detection, as well as internal processes and capabilities.

AI-powered detection tools are offered by a growing number of providers. Effective solutions need to provide the following: they can identify fabricated content, monitor social media for coordinated inauthentic behaviour targeting brands or executives, and flag anomalous narratives early.

Equally important are **internal protocols**:

- A senior leader should own disinformation risk, which ensures clear-cut accountability and a coordinated organisational response in case of an incident.
- Other proactive internal processes include multi-factor authentication and dual-authorisation policies for significant financial transactions.
- Perhaps most importantly, **training staff** to be sceptical of unexpected requests is central. Tabletop exercises, red teaming, and scenario planning to simulate disinformation attacks help test resilience. The development of a contextualised product that teaches employees about financial disinformation can be particularly effective. The introduction of these courses in the workplace can make a huge difference in preparedness levels, especially considering that human error is the main cause of companies becoming victims of cyberattacks.[31]

Practical guidance already exists to help governments, industry, and civil society manage disinformation crises proactively and reactively, such as the *AI Information Threats and Crisis Response: Practitioners' Handbook* by the Alan Turing Institute.[32]

Medium Term: Regulatory Reform. Effective policy solutions need to be quick and flexible enough to counter the threat. This can be ensured by focusing on the following priority areas identified by the CCOD:

- Statutory and regulatory changes targeting the spread of synthetic content online as well as the 'filter bubbles' and responsibilities of social media platforms. This includes **establishing strengthened powers to hold social media platforms accountable** for the disinformation amplified by their algorithms. One such

[31] Gregory, J. (2025). *CISOs list human error as their top cybersecurity risk*. IBM.
[32] Available at https://cetas.turing.ac.uk/publications/ai-information-threats-and-crisis-response-practitioners-handbook

measure should be **greater algorithmic transparency** to expose how platforms may indirectly profit from engagement driven by false or misleading content.

- **Removing financial incentives** for spreading disinformation; for example, research by Jon Roozenbeek highlights how low-cost SIM card farming (notably, the UK is the second-cheapest place to do so after Russia) enables large-scale evasion of platform verification systems, making coordinated manipulation both cheap and scalable.[33]
- **Expanding existing regulatory frameworks** (such as the UK's Cyber Security and Resilience Bill) to ensure that organisations designated as critical national infrastructure proactively **invest in preparedness against disinformation threats**, given the potential for significant economic and market disruption if targeted.
- **Increasing awareness and sharing of best practices**. This is the role of convening bodies like the CCOD to get together the countering disinformation ecosystem to share lessons, promote research and advocate for pragmatic solutions.

Medium- to long-term: Media Literacy and Digital Resilience. Education initiatives addressing the root causes of disinformation – the lack of digital and information skills – is the most effective way to become digitally resilient as a society. The CCOD calls for:

- **Increased funding for media literacy initiatives** with a specific focus on financial disinformation, including supporting programmes run by civil society organisations and the Department for Science, Innovation and Technology (DSIT). Funding can be increased through a voluntary or statutory levy on UK revenues of social media platforms, keeping the cost for the taxpayer low and ensuring platforms are held accountable for the spread of disinformation.
- Comprehensive curriculum reform, **embedding media literacy in primary and secondary education**. Instilling critical thinking skills and verification habits from a young age is both a personal skill and a civic responsibility. The CCOD is encouraged that the Education Curriculum Review suggests media literacy will be taught as early as 2027, and supports the development of a broader digital literacy strategy across all age groups. Alongside media literacy, the CCOD also calls for **digital resilience training**, including targeted education on resisting misinformation, disinformation, extremist content, misogynistic material, and other forms of harmful online influence.

[33] Centre for Science and Policy, University of Cambridge. (2025, July 18). *Disinformation, security and democracy*.

- A media literacy tool specifically designed for **workforces**: a scalable, contextualised programme that equips employees to recognise and respond to financial disinformation, including deepfake impersonation attacks.
- Increased **convening and knowledge-sharing** through bodies like the CCOD, bringing together the counter-disinformation ecosystem to exchange lessons, promote research and advocate for and deliver pragmatic, evidence-based solutions — from workforce media literacy to executive-level training — so organisations are prepared from top to bottom.

5. Conclusion

Financial disinformation is regrettably here to stay. Advances in generative AI mean the threat can expand both in scale — through fake reviews, AI-generated images and 'flooding the zone' tactics — and in sophistication, through targeted impersonation and precisely timed market manipulation.

The consequences are costly. Worldwide, disinformation has produced a $417 billion global economic cost. An engineering giant was defrauded of $25 million by a faked video call. A $209 billion bank was destroyed in 48 hours by social media panic. A publicly listed company lost 39% of its value in a single day due to a deliberately fabricated report.

The CCOD believes the areas where financial disinformation can have the greatest impact include reputational risk, market manipulation, risk to credit ratings, and scaled and accelerated cybercrime. A blend of reactive and proactive interventions will be best placed to meet this challenge. AI detection technology coupled with workforce media literacy tools will help protect businesses from the most acute threats. Looking ahead, investment in media literacy from a young age and systematic collection of best practice will enable us to build the digital resilience necessary to respond to the long-term threat posed by financial disinformation.

About us

The CCOD is a mission-led organisation fighting against online disinformation. We have two primary goals that define who we are, what we do, and what we stand for:

1) We aim to influence the policy and regulatory environment to ensure that the UK government effectively tackles the growing issue of online misinformation and disinformation. CCOD has helped convene a cross-party group of parliamentarians and works directly with policymakers to improve understanding of disinformation threats. We educate policymakers on disinformation challenges and work with them on workable policy, regulatory and legislative initiatives to protect online information integrity in the UK.

2) Our objective is to bring together the key actors working across the information integrity ecosystem, ranging from technology developers and researchers to civil society organisations and media specialists, and ensure that those at the forefront of developing innovative solutions to online disinformation are given a prominent voice in shaping public policy outcomes. In parallel, we support organisations in protecting themselves and their workforces from disinformation risks with our advisory services, helping to safeguard markets, economic stability, and public trust.

Our collaborators and partners have included RUSI, the Aspen Institute, the Alan Turing Institute, Adobe, Egregious, Refute, Schillings, Ghost Shift, and academics from the University of Cambridge, UCL, and LSE. Our work has been featured on Times Radio, Politico and PoliticsHome.

Our research and policy thinking is supported by a world-class advisory board, which includes, among others, John Penrose (former MP and Government Minister); Professor Sander van der Linden (Professor of Social Psychology at the University of Cambridge); Matthew Wicker (Assistant Professor at Imperial College and Research Associate at the Alan Turing Institute); Joseph Brandifino (Leads Policy Strategy at Scale AI); Naomi Krieger Carmy (VP Portfolio Management at the DeepTech VC fund Earth & Beyond Ventures); Clare Rewcastle Brown (award-winning investigative journalist); and a former Chair of Ofcom.

Publisher
Council for Countering Online Disinformation (CCOD)

Authors
Barbara Waldner, Tommaso Rabitti

Editors
Thomas Barton, James Rice

Design, layout and production
Barbara Waldner, James Rice

© 2026 Council for Countering Online Disinformation

Website: https://ccod.co.uk/