Hedge Funds News, April 2024

We will start with the revised version 2024 of the Guidance on Arrangements to Support Operational Continuity in Resolution, from the Financial Stability Board.

This guidance was originally published on 18 August 2016. A supplementary note has now been added to the original guidance.

Critical shared services, such as information technology infrastructure and software-related services, are necessary to support the continued provision of a financial institution's critical functions.

The FSB Guidance on Arrangements to Support Operational Continuity in Resolution sets out arrangements to support the continuity of those services in the event of resolution.

The guidance assists supervisory and resolution authorities and financial institutions to evaluate whether financial institutions that are subject to resolution planning requirements have appropriate arrangements to support operational continuity if the firm enters resolution.

It covers legal, contractual and governance frameworks, resourcing, management information systems and financial resources. As part of the digitalisation of the financial services sector, financial institutions have increased their dependencies

on third-party service providers in supporting critical shared services in recent years.

Guidance on Arrangements to Support Operational Continuity in Resolution

Revised version

This can bring multiple benefits to financial institutions, including flexibility, innovation and improved operational resilience.

However, if not properly managed, disruption to critical shared services could affect the continued provision of critical functions, posing risks to orderly resolution and, in some cases, financial stability.

The 2016 Guidance has been issued to include a supplementary note on the digitalisation of critical shared services as an addendum.

The supplementary note does not create any new guidance or requirements.

Rather, it specifies, for each section of the 2016 Guidance, how authorities and firms should think about the continuity of critical shared services in resolution when those services are digital.

Table of Contents

Guidance on Arrangements to Support Operational Continuity in Resolution (2016) *1*
1. Introduction 1
2. The concept of operational continuity 3
Critical shared services and critical functions 3
Operational continuity as a going concern supervisory consideration 4
3. Service delivery models and resolvability 5
Provision of services within a regulated legal entity 5
Provision of services by an intra-group service company 6
Provision of services by a third-party service provider 6
4. Possible arrangements to support operational continuity 7
Contractual provisions 9
Resolution strategies and post-stabilisation restructuring 10
Cross-border provision of shared services 11
Annex: Indicative information requirements to facilitate operational continuity 12
Supplementary note (2024) *15*
Digitalisation of critical shared services: Implementing the FSB Guidance on Arrangements to Support Operational Continuity in Resolution 15

To read more: https://www.fsb.org/wp-content/uploads/P180324.pdf

Commission sends request for information to LinkedIn on potentially targeted advertising based on sensitive data under Digital Services Act

European Commission

The European Commission has formally sent LinkedIn a request for information under the Digital Services Act (DSA), asking for more details on how their service complies with the prohibition of presenting advertisements based on profiling using special categories of personal data.

LinkedIn must provide the requested information by 5 April 2024. Based on the assessment of LinkedIn's reply, the Commission will assess next steps.

A request for information is an investigatory act that does not prejudge potential further steps the Commission may or may not decide to take. However, pursuant to Article 74 (2) of the DSA, the Commission can impose fines for incorrect, incomplete, or misleading information in response to a request for information.

Main establishment of the provider in the EU	**LinkedIn Ireland Unlimited Company**
Designated service	**LinkedIn**
Type of service under DSA	Very large online platform
Average monthly active users in millions*	Logged-in active users: 45.2 Logged-out site visits: 132.5
Digital Services Coordinator as of 17 February 2024	Ireland
DSA enforcement actions	• 25.04.2023: designation (Commission decision .pdf; press release) • 18.01.2024: request for information (press release) • 14.03.2024: request for information (press release)

Following the designation as a very large online platform in April 2023, LinkedIn is required to comply with the full set of provisions introduced by the DSA, including the obligation to enable users to identify basic information about the nature and origins of an advertisement and the ban on presenting advertisements based on profiling using special categories of personal data, such as sexual orientation, political opinions, or race.

This enforcement action is based on a complaint submitted to the Commission by civil society organisations: https://edri.org/our-work/civil-society-complaint-raises-concern-that-linkedin-is-violating-dsa-ad-targeting-restrictions/

To read more: https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-linkedin-potentially-targeted-advertising-based-sensitive-data#:~:text=The%20European%20Commission%20has%20formally,special%20categories%20of%20personal%20data.

Stronger Fraud Risk Management Could Improve the Integrity of the Trademark System

United States Government Accountability Office
Report to Congressional Committees

What GAO Found

The Trademark Modernization Act of 2020 (TMA) established two new procedures—expungement and reexamination—that allow individuals and businesses to challenge a registered trademark on the basis that it was not used in commerce, as is normally required. A successful challenge results in the trademark being removed from the register, thus making it available for potential use for the challenger or other applicants.

GAO found that from December 2021 through June 2023 the U.S. Patent and Trademark Office (USPTO) and attorneys representing trademark owners filed nearly 500 petitions under the new procedures.

Fraudulent Images of the Same Flashlight with Different Logos Included in Trademark Applications Submitted to USPTO

Source: GAO adaptation of U.S. Patent and Trademark Office images. | GAO-24-106533

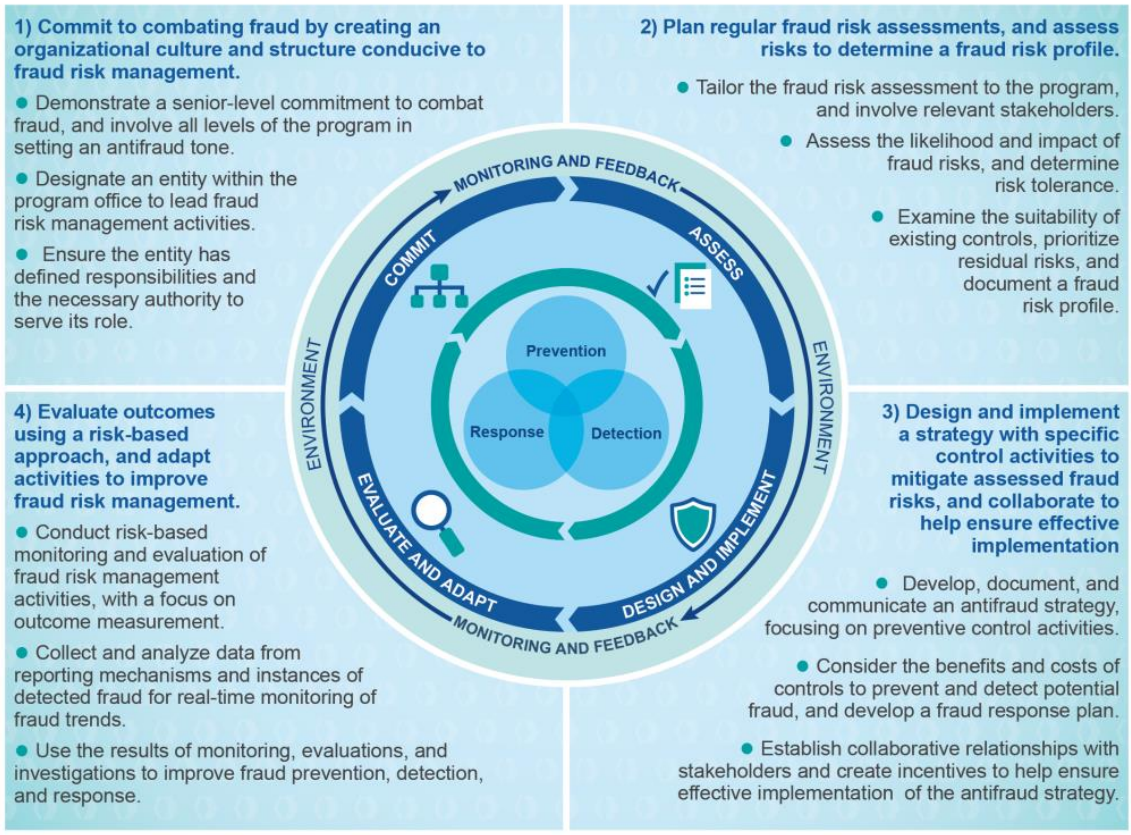
Collectively, these petitions resulted in the removal of more than 2,500 falsely claimed goods and services from the trademark register. Trademark attorneys told GAO that the new procedures can be cost-effective and low-risk.

Existing USPTO programs have also addressed inaccurate or false trademark applications and registrations. The agency's post registration audit program removed trademarked goods and services in about half of its randomly selected audits each year from the start of the program in 2017. This suggests that there may be more than 1 million false and inaccurate registrations out of about 2.8 million overall due to an influx of applications, among other factors.

The USPTO has taken steps to limit fraud risks, such as establishing a culture conducive to fraud risk management. However, the USPTO has not conducted a comprehensive fraud risk assessment of the trademark register or designed a fraud risk strategy. Implementing leading practices from GAO's Fraud Risk Framework would allow the USPTO to comprehensively consider fraud risks,

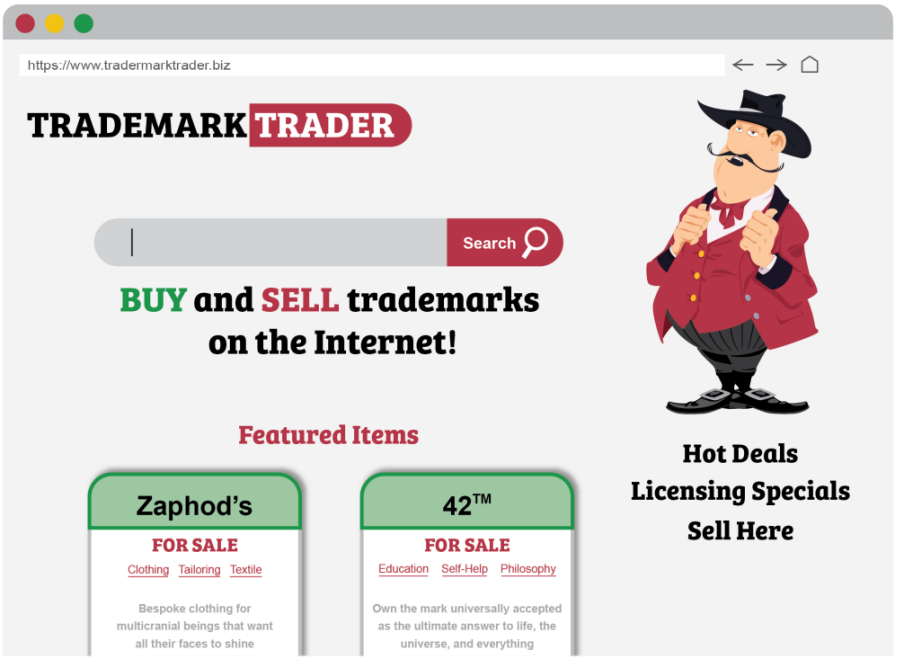
establish more effective controls, and fully articulate a tolerable level of fraud risk while considering the costs and benefits of potential control activities.

Figure 3: GAO Fraud Risk Management Framework



Source: GAO (information and icons). | GAO-24-106533

Figure 8: Illustrative Example of a Fictitious Trademark Auction Site



Source: GAO (data); Alexandr Sidorov/stock.adobe.com (images). | GAO-24-106533

GAO also found that the USPTO's current data systems do not allow the agency to:

(1) assess the effectiveness of current trademark fraud prevention programs and

(2) implement new technologies for identifying fraud.

Academics told GAO that computational tools such as predictive analytics could help the USPTO identify trademark applications with false or inaccurate information more effectively.

To read more: https://www.gao.gov/assets/d24106533.pdf

Digital finance - does it change the trade-off between risk and resilience?

Prof Claudia Buch, Chair of the Supervisory Board of the European Central Bank, at "The Future of Digitalization and Finance" symposium, organised by the Deutsche Bundesbank, Frankfurt am Main.

Thank you very much for organising this symposium on “The Future of Digitalization and Finance”. I am very grateful and honoured that it coincides with the farewell event for Joachim Wuermeling and me. I would like to thank the distinguished panellists for accepting the invitation to speak here today and I would like to thank all of you for coming.

First and foremost, I would like to thank all the dear colleagues here at the Bundesbank with whom I have worked closely over many years. Our work together has shaped my thinking about the banking and financial system, financial stability, the key role of our institutions in Europe and beyond, and the essential role of central banks in contributing to financial stability and the welfare-enhancing integration of financial markets. In today’s uncertain world, this is more important than ever.

I would like to thank you wholeheartedly for the great cooperation, and I am proud of what we have achieved together.

But the almost ten years that I spent at the Bundesbank as its Vice-President were in fact neither the beginning nor the end of our cooperation. Since the early 2000s, I have worked closely with the Bundesbank on many research projects, and in my new role as Chair of the Supervisory Board of the ECB, I will continue to work with all of you.

Dealing with today’s topic – the implications of digitalisation and its impact on the stability of banks – remains our joint responsibility within the Eurosystem.

Today’s banks operate in an environment which looks radically different to how it looked 30 years ago, due in no small part to the transformative impact of digitalisation.

The digital revolution, along with the rise of artificial intelligence, has the potential to fundamentally affect the key functions that banks perform in the economy.

Reducing information asymmetries, mitigating moral hazard, and leveraging their unique position to provide deposit-taking and lending services – these functions determine banks' franchise value and their role in the financial system.

This raises three important questions.

First, are we now witnessing a technological breakthrough in the provision of financial services? Remember what Paul Volcker said in 2009, "The most important financial innovation that I have seen the past 20 years is the automatic teller machine".

Second, how does digitalisation affect banks' risk/return trade-off? Does it lead to more competition and compression of margins, which induces a search for yield, which can in turn destabilise the financial system? Or are there counterbalancing forces that allow banks to better manage risks?

Third, what is the correct regulatory response to these trends? In my view, close cooperation across countries and sectors and addressing sources of systemic risk are key elements of the regulatory response.

We certainly won't be able to answer all these questions today, but I am very much looking forward to the panel discussion.

The changing landscape of competition in banking

The banking sector has undergone a significant transformation over the past 30 years. Let me highlight three shifts that have changed the landscape of competition in banking.

First, the internationalisation of banks has proceeded at a rapid pace. Let me give a European example. Today, international banks have a significant presence in central and eastern Europe, a development that was driven by deregulation and privatisation. This marks a stark contrast to the early 1990s when central and eastern European countries began opening up.

Historically, foreign banks primarily expanded overseas to follow their corporate customers. Outside of financial centres, their market shares were largely confined to trade-related business. But now, the landscape has transformed significantly; both international trade and international finance have seen considerable growth, facilitating the entry of foreign banks into new markets.

Second, banks are facing increased competition, particularly since the global financial crisis. This competition has come from non-bank financial institutions (NBFIs) such as investment funds, insurance companies and peer-to-peer lenders, but also from bigtech firms and fintech start-ups.

Several factors have driven this trend, including stricter regulation of banks and a growing demand for different or more innovative financial services. While bigtech firms have leveraged their massive user bases, technological expertise and data analytics capabilities to offer services, fintech start-ups have often been at the forefront of financial innovation.

Third, the digitalisation of financial services does indeed mark a pivotal point in the banking sector's development. The digital transformation is not just changing the types of services offered but it is also redefining how these services are

delivered and consumed. Digitalisation is changing the way in which financial services can be bundled together.

The key complementary services of the future may not be deposit taking and lending, but financial institutions may obtain a comparative advantage in terms of the information available from online commercial activity and social media. Digitalisation also reduces the cost of providing cross-border financial services, reducing the need for a physical presence in foreign markets, which may in fact benefit integration.

How does digitalisation affect the stability of banks?

What does the digitalisation of financial services imply for supervisors and regulators? Not only is the jury still out on whether digitalisation increases or decreases the degree of competition in the provision of financial services. There is also no clear answer as to how competition affects stability and how it affects the risk/return trade-off in the banking system.

On the one hand, forces that restrict competition may increase stability. Weak competition generates monopoly rents, which banks may want to protect by investing in safer assets.

On the other hand, instabilities may increase in less competitive markets, as banks with greater market power can set higher interest rates, which may lead to borrowers opting for riskier projects, thus resulting in banks becoming riskier.

Empirical studies actually show that the risk/return trade-off in banking depends on the types of risk (portfolio risk, insolvency risk, liquidity risk, systemic risk) and the business model being considered (retail versus wholesale banks).

How do the trends that we have seen over the past 30 years change the risk/return trade-off?

Let's take internationalisation first. The internationalisation of banking facilitates a more efficient diversification of risk. By operating across different countries, banks can spread their exposures over a wider array of economic environments and sectors.

International banking operations can achieve a more stable return on investments by leveraging this lack of perfect correlation between different markets. On the flip side though, the internationalisation of banking creates avenues for easier spillover of financial shocks from one country to another.

In a highly interconnected global banking network, stress in one country's banking sector can quickly affect financial institutions and markets in other countries. Shocks can ripple through the international banking system, affecting banks with exposure to that market through losses on investments or reduced confidence among depositors and investors.

The banking union that was established ten years ago is a response to the potentially adverse effects of integration and, at the same time, a channel through which sustainable integration can be enhanced.

The global financial crisis and the euro area sovereign debt crisis exposed significant vulnerabilities within the European banking sectors as well as the inadequacy of national supervisory frameworks to manage cross-border banking risks.

With the start of the Single Supervisory Mechanism (SSM) in 2014, whereby the ECB assumed direct supervision of significant banks in participating countries, common supervisory standards were established and enforced.

This ensures consistent supervision and a more holistic monitoring of the cross-border activities and exposures of banks within the SSM, supporting the integration of the European banking market. The ECB's Annual Report on Supervisory Activities 2023 provides insights into the measures taken to enhance the resilience of the European banking sector.

Changes in competition through the growth of NBFIs likewise affect the stability of banks, with both beneficial diversification of risks and the introduction of new channels of contagion. On the positive side, increased competition from NBFIs can lead to a more diversified financial system.

Diversification can spread risks across a wider array of institutions with different abilities to bear these risks. The system as a whole can become more resilient to shocks. However, competition from NBFIs introduces new vulnerabilities, particularly related to liquidity risk and high leverage, and it may increase incentives to take risk.

Reliance on short-term funding makes NBFIs susceptible to liquidity squeezes, whereby they may be forced to sell assets at depressed prices and potentially triggering a downward spiral in asset prices.

Furthermore, the interconnectedness between banks and NBFIs means that distress in the non-bank sector can quickly transmit to banks through direct exposures, common asset holdings, and market sentiment. An important way in which banks can mitigate this risk is by investing more in the assessment and management of the risks of their non-bank counterparties.

Finally, digitalisation affects risks and return in banking. On the one hand, digitalisation may expose banks to new risks such as cyberattacks and a high dependency on third-party providers.

Cyber threats can compromise data integrity, privacy and the overall operational continuity of banks. The ECB is currently conducting a cyber resilience stress test on 109 directly supervised banks to assess how banks respond to and recover from a cyberattack.

Similarly, dependency on a limited number of technology providers for critical services can introduce significant systemic risks if any of these providers fail or experience disruptions. The Digital Operational Resilience Act (DORA) thus provides supervisory authorities with more competences for the oversight and supervision of banks' outsourcing activities.

On the other hand, a higher concentration within the financial sector, often a consequence of digital transformation, may imply higher profitability and the ability to build larger buffers against risks. Moreover, by cooperating with fintech firms and integrating innovative solutions, banks may also benefit from a more efficient provision of their financial services.

Regulatory responses to the digitalisation of financial services

The current prudential framework for the regulation of banks is designed to be technologically neutral, recognising that regulators and supervisors do not have superior knowledge to market participants regarding the most effective technological solutions. But this certainly does not imply that we should ignore technology. Instead, we need to understand the impact of digitalisation on risks in the financial system and respond to potentially destabilising forces.

Digitalisation certainly reinforces the need for policy and supervisory coordination, both across countries and sectors. Bank risks never stopped at borders, but the digitalisation of financial services certainly affects the speed and nature of shock transmission.

The Financial Stability Board (FSB), reinvigorated since the global financial crisis, thus plays a crucial role in coordinating international efforts to monitor and address the financial stability risks posed by digitalisation. Similarly, the Basel Committee on Banking Supervision (BCBS) has been instrumental in setting global standards for the prudential regulation of banks, adapting these standards to account for the digitalisation of financial services.

Both the FSB and the BCBS have established frameworks for the evaluation of regulatory policies, which are crucial for the accountability and transparency of supervisors and regulators. In Europe, the push for better coordination has led to significant progress towards a banking union as well as to the call for a capital markets union. Both a banking union and a capital markets union are essential steps in creating a more integrated and resilient financial system.

In this cooperation, systemic risks arising from digitalisation and from changes in the provision of financial services need to be addressed. After the global financial crisis, stricter regulations were imposed on banks to reduce the likelihood and impact of future crises.

The reforms aimed to bolster the resilience of banks by enhancing their capitalisation, thus enabling them to better absorb losses and reduce systemic risk. Reforms also tackled the "too-big-to-fail" issue by imposing higher capital requirements on large, systemically important banks and enhancing mechanisms

for their recovery and resolution, lessening the financial burden on taxpayers in case of bank failures.

We similarly need to address systemic risks arising from non-banks. NBFIs, much like banks, play a crucial role in the global financial ecosystem, engaging in activities that affect liquidity flows and market functioning both domestically and internationally.

Like banks, non-banks need sufficient resilience to reduce the likelihood of distress and to mitigate the amplification of shocks, taking a systemic perspective rather than focusing solely on individual institutions.

While crypto-assets are not systemically relevant at present due to their small market capitalisation, history teaches us to be vigilant. The task at hand for regulators involves a comprehensive assessment of potential future systemic risks, requiring preventive regulation to address these risks before they materialise.

This involves close monitoring, international cooperation to close regulatory gaps, and a concerted effort to prevent regulatory arbitrage. In this sense, the Markets in Crypto-Assets (MiCa) regulation is a key European response to the provision of crypto-related services.

Finally, an emerging challenge in the digital financial landscape is the blurring of lines between policy areas. Digital financial services often cut across traditional sectoral boundaries, combining elements of banking, investment and insurance services, etc.

Policies aimed at fostering innovation in financial technologies can thus have significant implications for several policy areas. Hence, prudential supervisors not only need to coordinate with each other, but also with competition authorities to understand the dynamic market forces at play.

This coordination is crucial for ensuring that the drive towards digitalisation and the resulting market concentration, not least due to the market power of third-party providers of financial services, do not undermine financial stability.

To read more:
https://www.bankingsupervision.europa.eu/press/speeches/date/2024/html/ssm.sp240322~7bbfe50962.en.html

Browse safely with real-time protection on Chrome

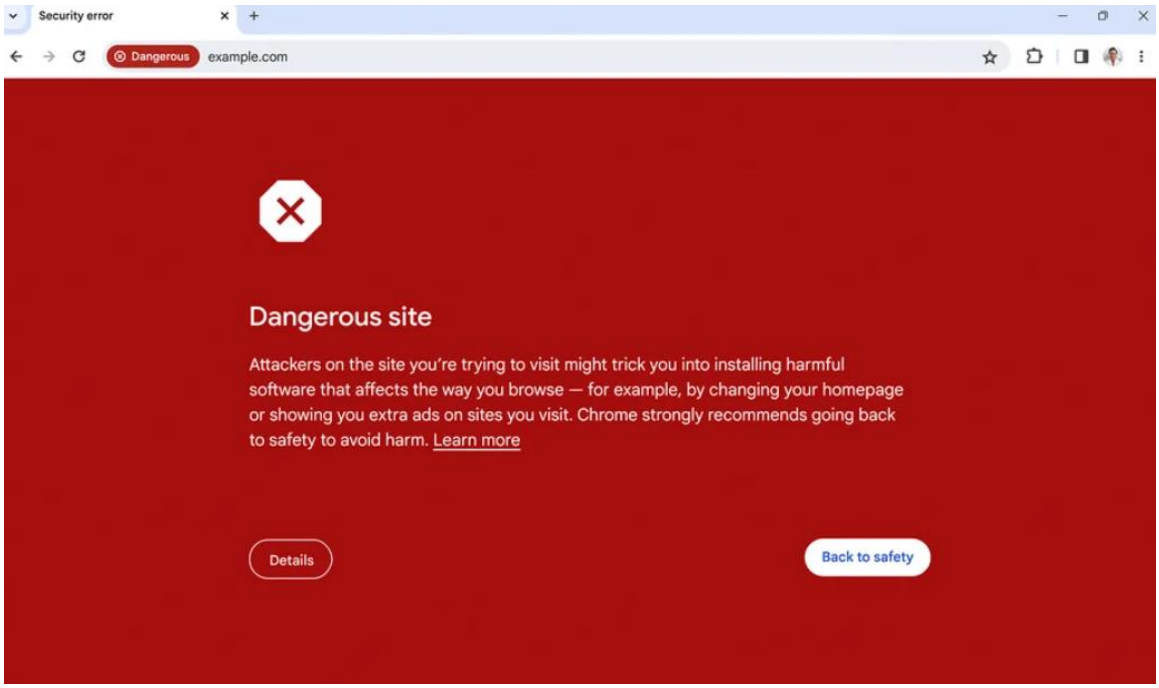
Google

Cybersecurity attacks are constantly evolving, and sometimes the difference between successfully detecting a threat or not is a matter of minutes. To keep up with the increasing pace of hackers, we're bringing real-time, privacy-preserving URL protection to Google Safe Browsing for anyone using Chrome on desktop or iOS. Plus we're introducing new password protections on Chrome for iOS as another way to help you safely navigate the web.

Real-time protection through Safe Browsing

Safe Browsing already protects more than 5 billion devices worldwide, defending against phishing, malware, unwanted software and more. In fact, Safe Browsing assesses more than 10 billion URLs and files every day, showing more than 3 million user warnings for potential threats.

Previously, the Standard protection mode of Safe Browsing used a list stored on your device to check if a site or file was known to be potentially dangerous. That list is updated every 30 to 60 minutes — but we've found that the average malicious site actually exists for less than 10 minutes.



So now, the Standard protection mode for Chrome on desktop and iOS will check sites against Google's server-side list of known bad sites in real time. If we suspect a site poses a risk to you or your device, you'll see a warning with more information. By checking sites in real time, we expect to block 25% more phishing attempts.

The new capability — also rolling out to Android later this month — uses encryption and other privacy-enhancing techniques to ensure that no one, including Google, knows what website you're visiting. While this does require some additional horsepower from the browser, we've worked to make sure your experience remains smooth and speedy.

If you want even more protection, you can always turn on Safe Browsing's Enhanced Protection mode, which uses AI to block attacks, provides deep file scans and offers extra protection from malicious Chrome extensions.

To read more: https://blog.google/products/chrome/google-chrome-safe-browsing-real-time/

Taking into account climate and nature in monetary policy and banking supervision around the world

Frank Elderson, Member of the Executive Board of the ECB and Vice-Chair of the Supervisory Board of the ECB, at an event on climate-related financial risks hosted by the Banco Central do Brasil

Many thanks to the Banco Central do Brasil for inviting me here today. I am honoured to be speaking in Rio de Janeiro's botanical garden. It is home to more than 6,500 different species – just a fraction of the more than 130,000 species that are estimated to be found in Brazil, the most biodiverse country in the world. But even this little glimpse into Brazil's biodiversity is more than sufficient to appreciate the concept of natural capital and the tremendous value it represents.

At the same time, global heating and nature degradation are putting this natural capital at risk. And central banks and supervisors around the world recognise that this poses a serious threat to the stability of our economies and the robustness of our financial system.

Let me be clear from the outset: central banks and supervisors are not, and do not intend to be, policymakers in the area of climate and nature. It is governments that are responsible for climate and nature policies.

In my remarks today, I will explain why central banks and supervisors have no option but to take the ongoing climate and nature crises into account to deliver on their monetary policy and banking supervision mandates. And that is exactly what central banks and supervisors around the world are doing.

We at the European Central Bank (ECB) are not alone in this work, as can be seen from the work being done by the Banco Central do Brasil and most other central banks and supervisors around the world.

The relevance of climate and nature for central banks and supervisors
Human-induced global heating and nature degradation are scientifically established facts.

Their devastating consequences are becoming all the more apparent in the increasing number of hazards we are seeing around the world. We don't yet know exactly how the climate and nature crises will continue to unfold, partly because governments are taking mitigation and adaptation measures.

This uncertainty also means that we don't know exactly how the economy and the financial system will be affected. At the same time, analysis consistently shows the vital importance of climate and nature for central banks and supervisors.

First, whatever happens, the economic impact will be profound. If left unchecked, global heating and nature degradation will contribute to increased macroeconomic volatility as climate and nature events become more frequent and have a greater impact on the economy.

A successful transition to a green and sustainable economy, meanwhile, will require vast investment flows that will alter the way our economies function.

Second, the economic benefits of a timely transition far outweigh the costs, especially when considered against the alternative scenarios of doing nothing or doing too little too late.

Third, climate-related risks translate into financial risks. Early work by the Basel Committee on Banking Supervision (BCBS) shows that climate events are a driver of each traditional type of risk considered in the regulatory framework, from credit risk, liquidity risk and market risk to reputational and operational risk, including legal risk.

Floods, for example, could damage a company's production facility, which could affect its ability to repay a loan, in turn leading to higher credit risk for the bank that provided the loan. Or consider what might happen if your house is built in an area vulnerable to wildfires. Your home could fall in value, leaving the bank that granted you the mortgage with higher risk on its balance sheet.

And these financial risks are not related solely to climate change. Last year, when looking at more than 4.2 million individual companies that account for over €4.2 trillion in corporate loans, we found that nearly 75% of all bank loans in the euro area are to companies that are highly dependent on at least one ecosystem service.

Examples of these services include the products we obtain from ecosystems, such as food, drinking water, timber and minerals; protection against natural hazards; or carbon uptake and storage by vegetation.

If these ecosystem services continue to experience the level of degradation they are currently facing, the stability of individual financial institutions and the broader financial system will be at risk.

International standard-setting bodies driving global action

Recognising the relevance of climate and nature-related factors for the economy, including the financial system, international standard-setting bodies are increasingly turning their attention to this topic. This has resulted in substantial progress at the global level, although more work lies ahead of us.

For example, the BCBS has a dedicated Task Force on Climate-related Financial Risks, whose meeting this week is kindly hosted by the Banco Central do Brasil. Based on the work of this task force, the BCBS has taken concrete steps to incorporate climate-related financial risks into the Basel framework for the global prudential regulation of banks.

And progress has been made across all three pillars of the prudential framework: regulation, supervision and disclosures. On the topic of disclosures, late last year the BCBS issued a consultation paper on a proposed climate-related disclosure requirements framework, building on the work done in various other fora. The deadline for comments was two weeks ago and we are now carefully assessing the feedback received.

Meanwhile, there is also progress on nature-related risks. In view of the Brazilian G20 Presidency's priority to deepen work on sustainability-related risk, the Financial Stability Board (FSB) will this year complement its climate-related work with a stocktake of current and planned regulatory and supervisory initiatives regarding nature-related financial risks.

This may build on the work already done by the Central Banks and Supervisors Network for Greening the Financial System (NGFS). Last year the NGFS – which has 138 members worldwide, including the Banco Central do Brasil – published a conceptual framework to guide action by central banks and supervisors in the area of nature-related risks.

The work currently being done by the BCBS, the FSB and the NGFS will ultimately find its way to other international standard-setting bodies and translate into concrete practices by individual central banks and supervisors.

ECB measures to take climate and nature into account

Let me give you some examples of actions we have taken at the ECB.

In 2021 we unveiled an ambitious climate action plan covering macroeconomic modelling, financial stability monitoring, data collection, risk assessment capabilities and our monetary policy operations. Many of the actions we planned have now been delivered.

For instance, we have made significant progress in improving the models that we use in macroeconomic analysis supporting our monetary policy decisions.

Moreover, we have in place a methodology to tilt the purchase of corporate bonds towards issuers with a better climate performance – if we ever need to buy corporate bonds again in the future.

In the collateral framework for our lending operations, we only accept assets that comply with the relevant sustainability reporting requirements and we are looking at setting limits on the share of assets issued by entities with a large carbon footprint.

In the area of banking supervision, we have urged banks to ensure the sound management of climate and nature-related risks, using the supervisory expectations we published in 2020 as a starting point.

These expectations give guidance on how banks should integrate climate and nature-related risks into their strategy, governance and risk management.

It is very much consistent with the general supervisory principles that have been established by the BCBS.

Since the ECB first started discussing climate and nature-related risks with banks back in 2019, progress has undoubtedly been made. Banks have taken steps to integrate these risks into their strategy, governance and risk management.

Although at present none of the banks under our supervision fully meets all our expectations, each of our expectations has already been fulfilled by at least one bank.

It shows that progress is possible, and that it is not just taking place among a few banks, but across the board. This is good news, since we expect all banks under our supervision to be fully aligned with our supervisory expectations by the end of 2024.

We will enforce this final deadline as well as several interim deadlines. In fact, a number of banks under our supervision have already received binding requirements to remedy shortcomings by a certain date. If they do not comply, they will have to pay a penalty for every day that the shortcomings remain unresolved.

Building on the results achieved and progress made, earlier this year the ECB announced a new climate and nature action plan. It sets out concrete steps to consider how, within our mandate, we can further support the green transition, assess the physical impacts of climate change and explore the materiality of nature-related risks.

Moreover, when we completed a review of our operational framework for implementing monetary policy two weeks ago, we announced that climate change-related considerations will be incorporated into the design of future structural monetary policy operations.

Conclusion

Let me conclude.

The Amazon river is subject to the “Pororoca”, one of the largest tidal bores in the world. It is an enormous wave travelling from the mouth of the Amazon on the Atlantic coast up to 800 kilometres upstream.

The climate and nature crises are unfolding. Together they are overflowing the economy and the financial system, very much like the “Pororoca” overflows the Amazon basin. Even if mitigation and adaptation measures are taken, one thing is certain: the world, the global economy and the financial system will see profound change.

In the words of Brazilian author Paulo Coelho: “You drown not from plunging into the water, but from staying submerged in it.” Emerging from the climate and nature crises requires action from all authorities within their mandate. For

central banks and supervisors, this means taking climate and nature into account in the pursuit of their monetary policy and supervisory objectives. If they failed to do so, they would be failing on their mandate. The work that we are doing individually and collectively proves that we will not allow this to happen.

Thank you for your attention.

To read more:
https://www.ecb.europa.eu/press/key/date/2024/html/ecb.sp240327_1~000d88f066.en.html

Propelling 3D printing into the future - Printing stronger materials five times faster

3D printing has changed the world.

It's allowed the aerospace, medical, automotive, manufacturing and many other industries to customize parts and prototypes in ways they never could before. It has drastically increased flexibility and cost effectiveness while reducing waste and production time. But many 3D-printed materials aren't the strongest.

A team of chemists and materials scientists at Sandia hopes to change that.

They've developed a new printing process that prints stronger nonmetallic materials in record time, five times faster than traditional 3D printing.

"It opens up a whole new world of what you can build and what 3D materials can be used for," materials scientist Samuel Leguizamon said.

He led the team that developed SWOMP, which stands for Selective Dual-Wavelength Olefin Metathesis 3D-Printing. As indicated by its name, it uses dual-wavelength light, unlike the traditional printing process.

How 3D printing works

Traditionally, vat 3D printing is accomplished by irradiating a vat of photosensitive liquid resin in a desired pattern.

As the resin is exposed to light from beneath the vat, the resin cures and hardens into a polymer layer. The cured polymer is then lifted, and a new pattern is projected beneath to cure subsequent layers.

One challenge: As the polymer cures, it adheres to the previous layer and to the bottom of the vat. After each layer, the cured polymer must be slowly peeled from the vat to prevent damage, significantly slowing down the 3D printing process.

Fellow creator Leah Appelhans said it's kind of like baking cookies. "After you bake the cookies, you have to let them cool. If you were to try to peel the warm cookie off the cookie sheet, it's squishy and it breaks apart. The same thing would happen with a 3D printer if you tried to quickly print each layer. Your work would get deformed."

Samuel, Leah, former Sandian Jeff Foster and polymer scientist Alex Commisso came up with a way to cool the "cookies" quicker.

UV and blue light

The key is combining two lights. In this case, ultraviolet and blue light.

The team took inspiration from a technique known as continuous liquid interface printing along with a printing approach using dual-wavelength light for acrylic-based polymerizations.

With it, they created SWOMP.

“You are still printing layer by layer, but you are using a second wavelength of light to prevent polymerization at the bottom of the vat. So it doesn’t adhere to the bottom,” Samuel said. “That means you can lift the cured polymer part more quickly and speed up the printing process significantly.”

Making 3D materials stronger

But this new process isn’t just about efficiency. It’s about making 3D-printed materials stronger and more versatile. Most vat-polymerization-printed materials are acrylic-based, not the strongest material.

“It’s really hard to use these materials in things like aircraft and space and aerospace and automotive. They are very harsh environments,” Sandia licensing executive Bob Sleeper said.

This team turned to the material dicyclopentadiene, which is commonly used in the production of paints, varnishes and flame retardants for plastics. They were able to develop a way to polymerize it more rapidly with light so that it can be used more efficiently in 3D printing.

“We changed building blocks of the materials from acrylic-based to olefin-based,” Samuel said. “Which lets us print materials that are a lot tougher.”

“That is the beauty of what they are doing,” Bob said. “You have very high-quality plastic parts that are made very precisely by using some light in a very novel way.”

Opening a new world of 3D printing

This team hopes their new printing process will open the world of 3D printing.

While the project was initially funded through a rapid three-month Exploratory Express program, it’s now funded by a Sandia technology maturation program.

“What we are trying to do is build the toolbox of materials available,” Leah said. “We want designers, researchers, engineers to be able to select the type of material they want to use.”

One day, they hope to see these 3D-printed parts in rockets, engines, batteries, maybe even in fusion applications. Samuel said they’re already talking with researchers at Lawrence Livermore National Laboratory to explore applications. “It turns out that monomers are already used in fusion components. You don’t usually think of a polymer used in fusion, but it’s really cool and exciting potential.”

The team also sees a world where 3D printing can be done more easily in remote areas. “We’re looking at locations where machinery and parts are not readily available; like in space, on the moon or in the Middle East at a U.S. military base,” Bob said. “You can bring with you some lightweight materials and make whatever you need on the spot.”

Samuel, who grew up in the small town of Wagener, South Carolina, is also thinking of applications that could help closer to home.

“I have horses. I grew up in a rural area, my dad was a farrier, so I’m thinking of ways to make horseshoes for racehorses. They have to be impact-resistant, but by changing the material properties, stress can be better spread out, and impact in the right space on the hoof. You could think of it as insoles for horses.”

The possibilities are endless.

“I think what attracted me to chemistry in the first place is the potential to make something that has never existed before,” Leah said. “The fun thing about 3D printing is that you apply that chemical knowledge to something that has a very concrete outcome. Something you can see and hold in your hands.”

To read more: https://www.sandia.gov/labnews/2024/03/07/propelling-3d-printing-into-the-future/

Johns Hopkins APL and Navy Chart Next Steps to Accelerate 3D-Printing Advancements

Ever made a mistake while sketching or writing in permanent ink and wanted to adjust your work — or scrap the whole thing altogether and start again? If so, you've utilized in situ monitoring.

It's a technique used in a variety of industries to monitor the production of something in real time and ensure defect-free items. It's also become increasingly important in the field of additive manufacturing.

"In traditional manufacturing, such as welding, a real person is operating the equipment, and the welder can adapt as they go," explained Michael Presley, a manufacturing engineer and project manager at the Johns Hopkins Applied Physics Laboratory (APL) in Laurel, Maryland.

"In additive manufacturing, we currently have open-loop systems in which we set parameters and the machine begins manufacturing on its own. The machine can lay miles of welds without ever knowing if something goes wrong. By utilizing in situ monitoring technologies, we can spot those errors earlier if they arise and develop more efficient and accurate processes."

These monitoring technologies cover a range of sensing modalities: systems ranging from cameras to pyrometers and thermocouples (devices that measure temperatures); spectrometers (that measure wavelengths of light to identify chemicals and materials) tuned across the infrared, visible, ultraviolet and X-ray spectrums; displacement sensors; profilometers (that measure the roughness of a surface's finish); ultrasonic transducers (that generate or sense energy, often vibration); and even microphones — just to name a few.

This wide scope arises from the complexity of the additive manufacturing process. Engineers need systems that concurrently measure the temperature and surface behavior of a molten metal drop moving at meters per second across a build plate, the quality of the bulk material it leaves behind, and the system health of all the lasers, pumps, actuators and feedback controls used by the machine.

Anticipating an Urgent Need

Integrating the wide range of technologies at the heart of in situ monitoring is a large systems-engineering challenge — and one of increasing importance to the Navy's manufacturing base. While speaking on a panel in London, U.S. Air Forces in Europe Commander Gen. James Hecker said the U.S. stockpile of weapons and munitions is getting "dangerously low."

And to further support the Department of Defense's deterrence plans, the Navy plans to invest roughly $132 billion to acquire 12 Columbia-class submarines —

the largest and most complex submarines in Navy history. But a recent Government Accountability Office report noted there could be trouble delivering those ships on time.

To address these manufacturing challenges, the Navy is prioritizing the development and fielding of additive manufacturing systems, often called 3D printers, to supplement traditional casting methods and accelerate submarine production.

To support this effort, APL hosted a working group in July to discuss the current state of in situ monitoring in additive manufacturing, identify opportunities for advancement, and develop a path forward for future Navy implementation of such technology.

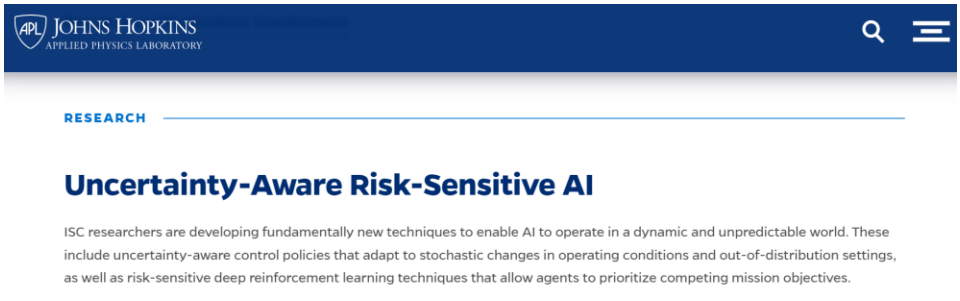
“Collaboration is going to be key in addressing both logistics and sustainment challenges in the current fleet and force and the manufacturing challenges of our future fleet and its weapon systems,” said James Borghardt, APL’s Maritime Expeditionary Logistics program manager. “We’re looking forward to our continued work with the Navy, Department of Defense and partner organizations to keep the field moving forward.”

The event was managed by team members from APL’s Force Projection Sector, Air and Missile Defense Sector, and Research and Exploratory Development Department with support from the Naval Sea Systems Command (NAVSEA 05T) and the Program Executive Office, Strategic Submarines.

Among the 32 participating organizations were the Applied Research Laboratory at Penn State University, Virginia’s Commonwealth Center for Advanced Manufacturing, America Makes, the Army Research Laboratory, Naval Air Systems Command, the Office of Naval Research, Oak Ridge National Laboratory, the Defense Logistics Agency, the Nuclear Regulatory Commission and a range of Naval Surface Warfare Centers.

“We went from having a few dozen people in the Navy studying and monitoring additive manufacturing capabilities to now having hundreds,” said Presley. “And we’re trying to bring everyone up to speed and move as fast as possible because these are real, near-term needs. In situ monitoring will play a vital role here because it can speed up and improve inspection of additive manufactured parts.”

To read more: https://www.jhuapl.edu/news/news-releases/240319b-apl-navy-chart-next-steps-for-3d-printing-advancements




APL
JOHNS HOPKINS
APPLIED PHYSICS LABORATORY
80
YEARS

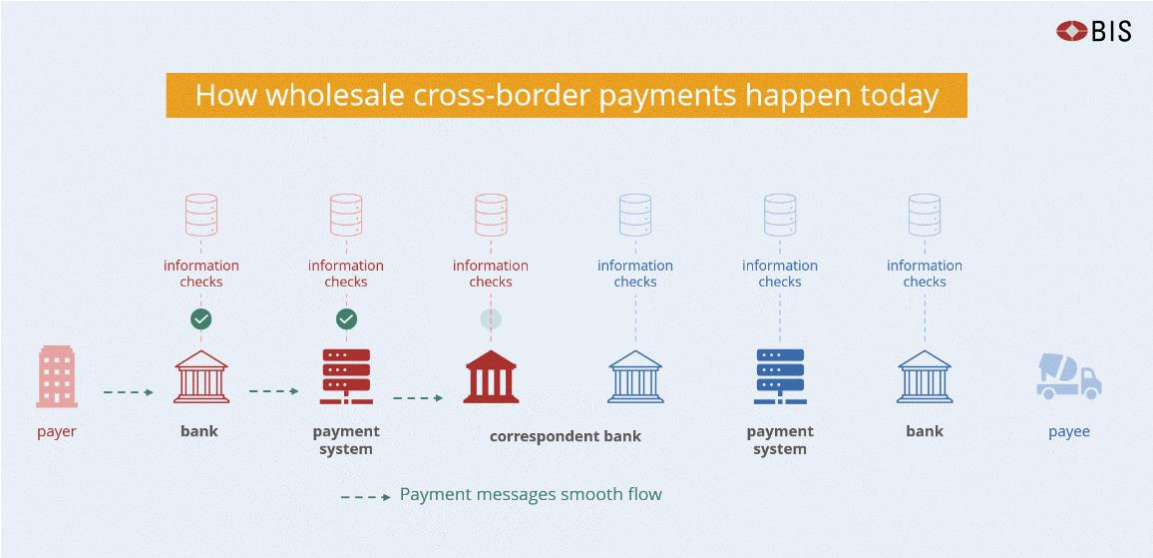
Project Agorá (Greek for "marketplace"): central banks and banking sector embark on major project to explore tokenisation of cross-border payments

The Bank for International Settlements (BIS) together with seven central banks today announced plans to join forces with the private sector to explore how tokenisation can enhance the functioning of the monetary system.

Project Agorá (Greek for "marketplace") brings together seven central banks: Bank of France (representing the Eurosystem), Bank of Japan, Bank of Korea, Bank of Mexico, Swiss National Bank, Bank of England and the Federal Reserve Bank of New York. They will seek to work in partnership with a large group of private financial firms convened by the Institute of International Finance (IIF).

The project builds on the unified ledger concept proposed by the BIS and will investigate how tokenised commercial bank deposits can be seamlessly integrated with tokenised wholesale central bank money in a public-private programmable core financial platform.

This could enhance the functioning of the monetary system and provide new solutions using smart contracts and programmability, while maintaining its two-tier structure.



Smart contracts can enable new ways of settlement and unlock types of transactions that are not viable or practical today, in turn offering new opportunities to benefit businesses and people.

This major public-private partnership will seek to overcome several structural inefficiencies in how payments happen today, especially across borders, which add a layer of challenges: different legal, regulatory and technical requirements, operating hours and time zones. Plus the increased complexity of carrying out

financial integrity controls (eg against money laundering and customer verification), which today are often repeated several times for the same transaction, depending on the number of intermediaries involved.

BIS Innovation Hub projects are generally experimental in nature and aim to explore and deliver public goods to the global central banking community.

Next steps

The BIS will issue a call for expressions of interest to private financial institutions to join Project Agorá. The IIF will act as the intermediary and convener of private sector participants.

It is envisaged that several regulated financial institutions will participate representing each of the seven currencies. Specific instructions and requirements will be issued in due course. Being a member of the IIF is not a requirement to participate.

To read more: https://www.bis.org/about/bisih/topics/fmis/agora.htm

Federal Reserve Board announces final rule that updates risk management requirements for certain systemically important financial market utilities (FMUs) supervised by the Board

FEDERAL RESERVE SYSTEM

12 CFR Part 234

Regulation HH; Docket No. R-1782

RIN No. 7100-AG40

Financial Market Utilities

AGENCY: Board of Governors of the Federal Reserve System

ACTION: Final rule

FMUs provide essential infrastructure to clear and settle payments and other financial transactions. Financial institutions, including banking organizations, participate in FMU arrangements pursuant to a common set of rules and procedures, technical infrastructure, and risk-management framework.

If a systemically important FMU fails to perform as expected or fails to effectively measure, monitor, and manage its risks, it could pose significant risk to its participants and the financial system more broadly.

For example, the inability of an FMU to complete settlement on time could create credit or liquidity problems for its participants or other FMUs.

An FMU, therefore, should have a robust risk-management framework, including appropriate policies and procedures to measure, monitor, and manage the range of risks that arise in or are borne by the FMU.

Title VIII of the Dodd-Frank Act, titled the "Payment, Clearing, and Settlement Supervision Act of 2010," was enacted to mitigate systemic risk in the financial system and to promote financial stability, in part, through an enhanced supervisory framework for designated FMUs.

Section 803(6) of the Act defines an FMU as a "person that manages or operates a multilateral system for the purpose of transferring, clearing, or settling payments, securities, or other financial transactions among financial institutions or between financial institutions and the person."

Pursuant to section 805(a)(1)(A) of the Act, and as described below, the Board is required to prescribe risk-management standards governing the operations

related to the payment, clearing, and settlement activities of certain designated FMUs.

The Board adopted Regulation HH, Designated Financial Market Utilities, in July 2012 to implement, among other things, the statutory provisions under section 805(a)(1)(A) of the Act.

In November 2014, the Board published amendments to the risk-management standards in Regulation HH based on the Principles for Financial Market Infrastructures (PFMI).

In October 2022, the Board published for comment a notice of proposed rulemaking (NPRM) to amend the requirements relating to operational risk management in Regulation HH.

The Board proposed to update, refine, and add specificity to the operational risk management requirements in Regulation HH.

The proposed amendments reflected changes in the operational risk, technology, and regulatory landscape in which designated FMUs operate since the Board last amended Regulation HH in 2014. The Board also proposed to adopt specific incident notification requirements.

The public comment period for the proposed amendments closed on December 5, 2022. The Board is now adopting final amendments to Regulation HH, with modifications to certain sections of the proposal as discussed below.

To read more:
https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20240308a1.pdf

According to Advocate General Priit Pikamäe, a database containing personal data may, under certain conditions, be sold in enforcement proceedings, even if the data subjects have not consented to the sale

COURT OF JUSTICE
OF THE EUROPEAN UNION

A Polish court is ruling on a dispute between a company and a member of the board of directors of another company that specialises in online sales and against which the first company has a debt claim.

That member may be personally liable where the debtor company does not have assets to satisfy the creditor company's claim. However, that member is of the opinion that this is not the case because the debtor company has, among other assets, two databases of users of the online platform it had created.

They contain personal data of hundreds of thousands of people who have not consented to the processing of their data in the form of making those data available to third parties outside that platform.

The Polish court has doubts as to whether the General Data Protection Regulation (GDPR) allows a court enforcement officer to sell those databases, in the context of enforcement proceedings, without the consent of the data subjects and has referred the matter to the Court of Justice.

In his Opinion, Advocate General Priit Pikamäe proposes that the Court should answer in the affirmative.

In his view, the operations carried out by the court enforcement officer for the purposes of estimating the value of the databases concerned and selling them by public auction come within the scope of the GDPR.

They include, at the very least, the retrieval, consultation, use and making available to the purchaser of those personal data and, consequently, must be regarded as a 'processing' of those data within the meaning of that regulation.

Furthermore, the Advocate General takes the view that the court enforcement officer must be regarded as the controller of the personal data.

Furthermore, the Advocate General concludes that the processing in question is lawful where it is necessary for the performance of a task carried out in the exercise of official authority vested in the court enforcement officer.

Lastly, the Advocate General notes that the purpose of the processing carried out by the court enforcement officer differs from the initial purpose of enabling the use of the online sales platform concerned.

In order for such further processing to be regarded as being compatible with the GDPR, it must constitute a necessary and proportionate measure in a democratic society to achieve one of the objectives of general interest pursued by that regulation.

According to the Advocate General, of those objectives, the objective of ensuring the enforcement of civil law claims may, in principle, justify the processing of the data at issue in the present case.

He also states that the assessment of whether a measure is proportionate, which the Polish court must carry out, involves balancing the creditor company's right to property and the right to protection of personal data of the users of the online platform concerned.

NOTE: The Advocate General's Opinion is not binding on the Court of Justice. It is the role of the Advocates General to propose to the Court, in complete independence, a legal solution to the cases for which they are responsible. The Judges of the Court are now beginning their deliberations in this case. Judgment will be given at a later date.

NOTE: A reference for a preliminary ruling allows the courts and tribunals of the Member States, in disputes which have been brought before them, to refer questions to the Court of Justice about the interpretation of EU law or the validity of an EU act. The Court of Justice does not decide the dispute itself. It is for the national court or tribunal to dispose of the case in accordance with the Court's decision, which is similarly binding on other national courts or tribunals before which a similar issue is raised.

Unofficial document for media use, not binding on the Court of Justice.

To read more: https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-02/cp240035en.pdf

https://curia.europa.eu/juris/documents.jsf?num=C-693/22

Commission fines Apple over €1.8 billion over abusive App store rules for music streaming providers

The European Commission has fined Apple over €1.8 billion for abusing its dominant position on the market for the distribution of music streaming apps to iPhone and iPad users ('iOS users') through its App Store.

In particular, the Commission found that Apple applied restrictions on app developers preventing them from informing iOS users about alternative and cheaper music subscription services available outside of the app ('anti-steering provisions'). This is illegal under EU antitrust rules.

The infringement

Apple is currently the sole provider of an App Store where developers can distribute their apps to iOS users throughout the European Economic Area ('EEA'). Apple controls every aspect of the iOS user experience and sets the terms and conditions that developers need to abide by to be present on the App Store and be able to reach iOS users in the EEA.

The Commission's investigation found that Apple bans music streaming app developers from fully informing iOS users about alternative and cheaper music subscription services available outside of the app and from providing any instructions about how to subscribe to such offers. In particular, the anti-steering provisions ban app developers from:

- Informing iOS users within their apps about the prices of subscription offers available on the internet outside of the app.
- Informing iOS users within their apps about the price differences between in-app subscriptions sold through Apple's in-app purchase mechanism and those available elsewhere.
- Including links in their apps leading iOS users to the app developer's website on which alternative subscriptions can be bought. App developers were also prevented from contacting their own newly acquired users, for instance by email, to inform them about alternative pricing options after they set up an account.

Today's decision concludes that Apple's anti-steering provisions amount to unfair trading conditions, in breach of Article 102(a) of the Treaty on the Functioning of the European Union ('TFEU'). These anti-steering provisions are neither necessary nor proportionate for the protection of Apple's commercial interests in relation to the App Store on Apple's smart mobile devices and negatively affect the interests of iOS users, who cannot make informed and effective decisions on

where and how to purchase music streaming subscriptions for use on their device.

Apple's conduct, which lasted for almost ten years, may have led many iOS users to pay significantly higher prices for music streaming subscriptions because of the high commission fee imposed by Apple on developers and passed on to consumers in the form of higher subscription prices for the same service on the Apple App Store.

Moreover, Apple's anti-steering provisions led to non-monetary harm in the form of a degraded user experience: iOS users either had to engage in a cumbersome search before they found their way to relevant offers outside the app, or they never subscribed to any service because they did not find the right one on their own.

Fine

The fine was set on the basis of the Commission's 2006 Guidelines on fines. In setting the level of the fine, the Commission took into account the duration and gravity of the infringement as well as Apple's total turnover and market capitalization. It also factored in that Apple submitted incorrect information in the framework of the administrative procedure.

In addition, the Commission decided to add to the basic amount of the fine an additional lump sum of €1.8 billion to ensure that the overall fine imposed on Apple is sufficiently deterrent.

Such lump sum fine was necessary in this case because a significant part of the harm caused by the infringement consists of non-monetary harm, which cannot

be properly accounted for under the revenue-based methodology as set out in the Commission's 2006 Guidelines on Fines. In addition, the fine must be sufficient to deter Apple from repeating the present or a similar infringement; and to deter other companies of a similar size and with similar resources from committing the same or a similar infringement.

The Commission has concluded that the total amount of the fine of over €1.8 billion is proportionate to Apple's global revenues and is necessary to achieve deterrence.

The Commission has also ordered Apple to remove the anti-steering provisions and to refrain from repeating the infringement or from adopting practices with an equivalent object or effect in the future.

Background to the investigation

In June 2020, the Commission opened formal proceedings into Apple's rules for app developers on the distribution of apps via the App Store. In April 2021, the Commission sent Apple a Statement of Objections, to which Apple responded in September 2021.

In February 2023 the Commission replaced the 2021 Statement of Objections by another Statement of Objections clarifying the Commission's objections, to which Apple responded in May 2023.

Procedural background

Article 102 of the TFEU and Article 54 of the European Economic Area Agreement prohibit the abuse of a dominant position.

Market dominance is, as such, not illegal under EU antitrust rules. However, dominant companies have a special responsibility not to abuse their powerful market position by restricting competition, either in the market where they are dominant or in separate markets.

Fines imposed on companies found in breach of EU antitrust rules are paid into the general EU budget. These proceeds are not earmarked for particular expenses, but Member States' contributions to the EU budget for the following year are reduced accordingly. The fines therefore help to finance the EU and reduce the burden for taxpayers.

In accordance with the EU-UK Withdrawal Agreement, the EU continues to be competent for this case, which was initiated before the end of the transition period (“continued competence case”) for the UK. The EU will reimburse the UK for its share of the amount of the fine collected by the EU once the fine has become definitive.

More information on this case will be available under the case number AT.40437 in the public case register on the Commission's competition website, once confidentiality issues have been dealt with.

Action for damages

Any person or company affected by anti-competitive behaviour as described in this case may bring the matter before the courts of the Member States and seek damages.

The case law of the Court of Justice of the European Union and Regulation 1/2003 both confirm that in cases before national courts, a Commission decision constitutes binding proof that the behaviour took place and was illegal.

Even though the Commission has fined the company concerned, damages may be awarded by national courts without being reduced on account of the Commission fine.

To read more:
https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1161

The U.S. Government Accountability Office (GAO)
COMBATING DEEPFAKES

GAO Science, Technology Assessment, and Analytics

WHY THIS MATTERS

Malicious use of deepfakes could erode trust in elections, spread disinformation, undermine national security, and empower harassers.

KEY TAKEAWAYS

- Current deepfake detection technologies have limited effectiveness in real-world scenarios.
- Watermarking and other authentication technologies may slow the spread of disinformation but present challenges.
- Identifying deepfakes is not by itself sufficient to prevent abuses. It may not stop the spread of disinformation, even after the media is identified as a deepfake.

Deepfakes are videos, audio, or images that have been manipulated using artificial intelligence (AI), often to create, replace, or alter faces or synthesize speech. They can seem authentic to the human eye and ear.

They have been maliciously used, for example, to try to influence elections and to create non-consensual pornography.

To combat such abuses, technologies can be used to detect deepfakes or enable authentication of genuine media.

Detection technologies aim to identify fake media without needing to compare it to the original, unaltered media.

These technologies typically use a form of AI known as machine learning.

The models are trained on data from known real and fake media.

Methods include looking for:

(1) facial or vocal inconsistencies,

(2) evidence of the deepfake generation process, or

(3) color abnormalities.

Authentication technologies are designed to be embedded during the creation of a piece of media. These technologies aim to either prove authenticity or prove that a specific original piece of media has been altered.

They include:

- Digital watermarks. They can be embedded in a piece of media, which can help detect subsequent deepfakes. One form of watermarking adds pixel or audio patterns that are detectable by a computer but are imperceptible to humans.

  The patterns disappear in any areas that are modified, enabling the owner to prove that the media is an altered version of the original. Another form of watermarking adds features that cause any deepfake made using the media to look or sound unrealistic.

- Metadata—which describe the characteristics of data in a piece of media—can be embedded in a way that is cryptographically secure. Missing or incomplete metadata may indicate that a piece of media has been altered.

- Blockchain. Uploading media and metadata to a public blockchain creates a relatively secure version that cannot be altered without the change being obvious to other users. Anyone could then compare a file and its metadata to the blockchain version to prove or disprove authenticity.

To read more: https://www.gao.gov/assets/d24107292.pdf

Internet Crime Report 2023

THE IC3

Today's FBI is an intelligence-driven and threat focused national security organization with both intelligence and law enforcement responsibilities.

We are focused on protecting the American people from terrorism, espionage, cyber-attacks, and major criminal threats which are increasingly emanating from our digitally connected world.

To do that, the FBI leverages the IC3 as a mechanism to gather intelligence on internet crime so that we can provide the public and our many partners with information, services, support, training, and leadership to stay ahead of the threat.

The IC3 was established in May 2000 to receive complaints crossing the spectrum of cyber matters, to include online fraud in its many forms including Intellectual Property Rights (IPR) matters, Computer Intrusions (Hacking), Economic Espionage (Theft of Trade Secrets), Online Extortion, International Money Laundering, Identity Theft, and a growing list of Internet-facilitated crimes.

As of December 31, 2023, the IC3 has received over eight million complaints.

The IC3's mission is to provide the public and our partners with a reliable and convenient reporting mechanism to submit information concerning suspected cyber enabled criminal activity and to develop effective alliances with law enforcement and industry partners to help those who report.

Information is analyzed and disseminated for investigative and intelligence purposes for law enforcement and public awareness.

The information submitted to the IC3 can be impactful in the individual complaints, but it is most impactful in the aggregate.

That is, when the individual complaints are combined with other data, it allows the FBI to connect complaints, investigate reported crimes, track trends and threats, and, in some cases, even freeze stolen funds.

Just as importantly, the IC3 shares reports of crime throughout its vast network of FBI field offices and law enforcement partners, strengthening our nation's collective response both locally and nationally.

To promote public awareness and as part of its prevention mission, the IC3 aggregates the submitted data and produces an annual report on the trends impacting the public as well as routinely providing intelligence reports about trends.

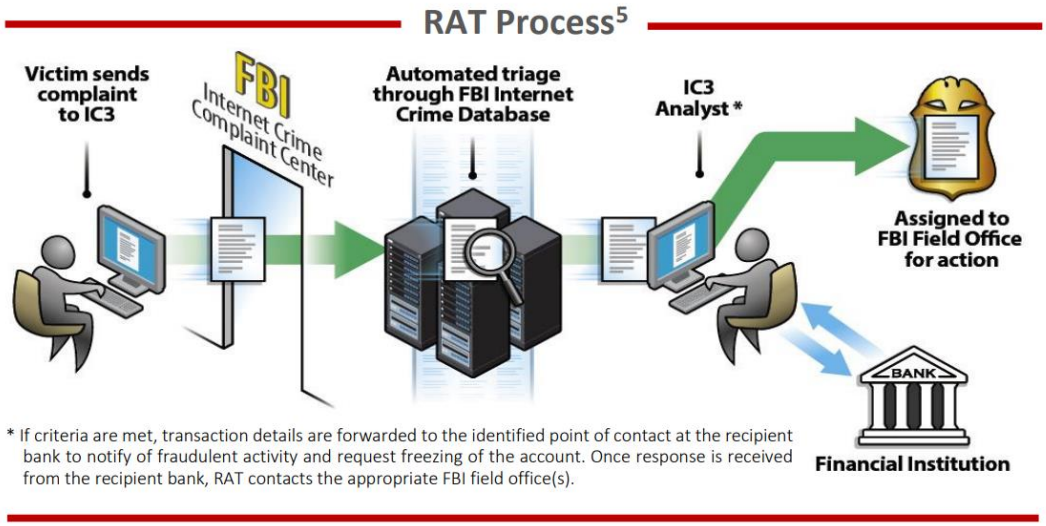
The success of these efforts is directly related to the quality of the data submitted by the public through the www.ic3.gov interface. Their efforts help the IC3, and the FBI better protect their fellow citizens.

2023 CRIME TYPES

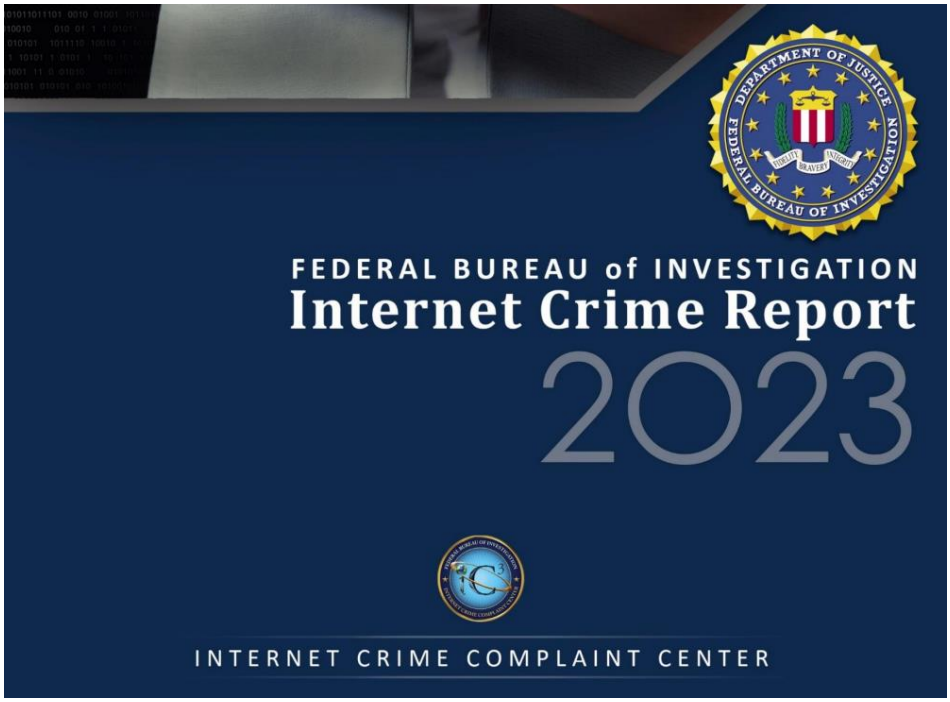
By Complaint Count			
Crime Type	*Complaints*	*Crime Type*	*Complaints*
Phishing/Spoofing	298,878	Other	8,808
Personal Data Breach	55,851	Advanced Fee	8,045
Non-payment/Non-Delivery	50,523	Lottery/Sweepstakes/Inheritance	4,168
Extortion	48,223	Overpayment	4,144
Investment	39,570	Data Breach	3,727
Tech Support	37,560	Ransomware	2,825
BEC	21,489	Crimes Against Children	2,361
Identity Theft	19,778	Threats of Violence	1,697
Confidence/Romance	17,823	IPR/Copyright and Counterfeit	1,498
Employment	15,443	SIM Swap	1,075
Government Impersonation	14,190	Malware	659
Credit Card/Check Fraud	13,718	Botnet	540
Harassment/Stalking	9,587		
Real Estate	9,521		

THE IC3 RECOVERY ASSET TEAM (RAT)

The Internet Crime Complaint Center's Recovery Asset Team (RAT) was established in February 2018 to streamline communication with financial institutions and assist FBI field offices with the freezing of funds for those who made transfers to domestic accounts under fraudulent pretenses.



To read more:
https://www.ic3.gov/media/pdf/annualreport/2023_ic3report.pdf



Disclaimer

The International Association of Hedge Funds Professionals (IAHFP)(hereinafter "Association") enhances public access to information. Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

The Association expressly disclaims all warranties, either expressed or implied, including any implied warranty of fitness for a particular purpose, and neither assumes nor authorizes any other person to assume for it any liability in connection with the information or training programs provided.

The Association and its employees will not be liable for any loss or damages of any nature, either direct or indirect, arising from use of the information provided, as these are general information, not specific guidance for an organization or a firm in a specific country.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;

- should not be relied on in the particular context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which the Association has no control and for which the Association assumes no responsibility;

- is not professional or legal advice;

- is in no way constitutive of interpretative;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including court rulings, were to lead it to revise some of the views expressed here;

- does not prejudge the interpretation that the courts might place on the matters at issue.

We are not responsible for opinions and information posted by others. The inclusion of links to other web sites does not necessarily imply a recommendation or endorsement of the views expressed within them. Links to other web sites are presented as a convenience to users. The Association does not accept any responsibility for the content, accuracy, reliability, or currency found on external web sites.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts. It is our goal to minimize disruption

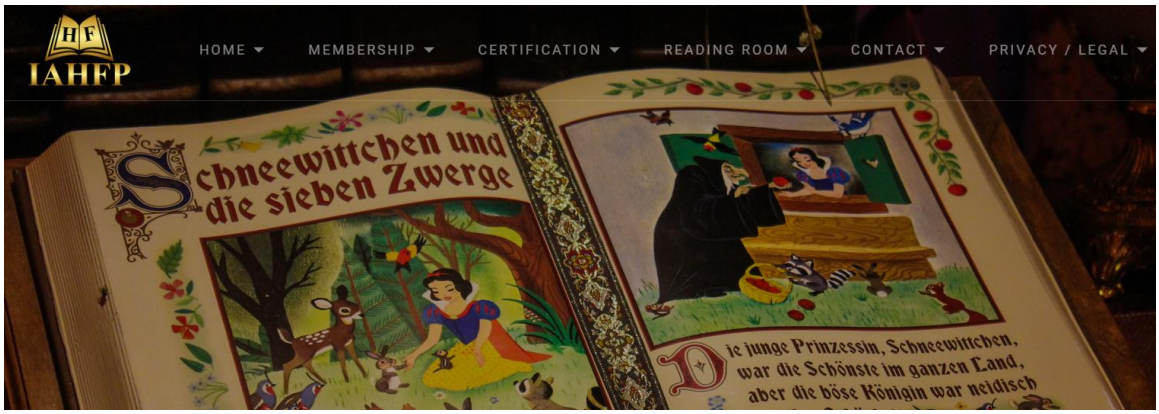
caused by technical errors. However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems. The Association accepts no responsibility with regard to such problems incurred as a result of using this site or any linked external sites.

Readers that are interested in a specific topic covered in the newsletter, must download the official papers, must find more information, and must ask for legal and technical advice, before making any business decisions.

International Association of Hedge Funds Professionals (IAHFP)

The Association is a business unit of Compliance LLC, incorporated in Wilmington, NC, and offices in Washington, DC, a provider of risk and compliance training in 57 countries.

Our reading room:
https://www.hedge-funds-association.com/Reading_Room.htm



“Mirror, mirror on the wall, who in this land is fairest of all?”

Children’s fiction can open up new perspectives for adults. Black swan events, exercising (or failing to exercise) the zero trust principle, risks and opportunities are all there.

Investigating the facts is the next pleasure. In 1994, Eckhard Sander claimed that the character of Snow White was based on the life of Margaretha von Waldeck, a German countess born in 1533. At the age of 16, Margaretha was forced by her stepmother, Katharina of Hatzfeld, to move away to Brussels. There, Margaretha fell in love with a prince who would later become Philip II of Spain.

Graham Anderson compares the story of Snow White to the Roman legend of Chione, recorded in Ovid's Metamorphoses. The name Chione means "snow" in Greek and, in the story, she is described as the most beautiful woman in the land, so beautiful that the gods Apollo and Hermes both fell in love with her.

For Snow White, the death of her real mother and the arrival of a stepmother is a disaster. Snow White is forced to leave home, but she discovers who she is, and moves along the path to self-discovery and resilience. This is a story about development set in motion by the arrival of evil. Does it look familiar?

Contact Us

Lyn Spooner
Email: lyn@hedge-funds-association.com

George Lekatis
President of the IAHFP

1200 G Street NW Suite 800,
Washington DC 20005, USA
Email: lekatis@hedge-funds-association.com
Web: www.hedge-funds-association.com
HQ: 1220 N. Market Street Suite 804,
Wilmington DE 19801, USA