International Association of Potential, New and Sitting Members
of the Board of Directors (IAMBD)
1200 G Street NW Suite 800, Washington DC, 20005-6705 USA
Tel: 202-449-9750 Web: www.iambd.org

News for the Board of Directors, May 2023

Dear members and friends,

We have a very interesting final report from the Financial Stability Board (FSB), with title: "Recommendations to Achieve Greater Convergence in Cyber Incident Reporting".

Executive summary

Cyber incidents are rapidly growing in frequency and sophistication. At the same time, the cyber threat landscape is expanding amid digital transformation, increased dependencies on third party service providers and geopolitical tensions.

The interconnectedness of the global financial system makes it possible that a cyber incident at one financial institution (FI) (or an incident at one

of its third-party service providers) could have spill-over effects across borders and sectors.

Recognising that timely and accurate information on cyber incidents is crucial for effective incident response and recovery and promoting financial stability, the G20 asked the FSB to deliver a report on achieving greater convergence in cyber incident reporting (CIR).

Table of Contents

To meet this call, the FSB conducted work to promote greater convergence in CIR in three ways:

(i) setting out recommendations to address the issues identified as impediments to achieving greater harmonisation in incident reporting;

(ii) enhancing the Cyber Lexicon1 to include additional terms related to CIR as a ‘common language’ is necessary for increased convergence; and

(iii) identifying common types of information that are submitted by FIs to authorities for CIR purposes, which culminated in a concept for a common format for incident reporting exchange (FIRE) to collect incident information from FIs and use between themselves.

FIRE would be flexible to allow a range of adoption choices and include the most relevant data elements for financial authorities.

Drawing from the FSB's body of work on cyber, including engagement with external stakeholders, this report sets out recommendations that aim to promote convergence among CIR frameworks, while recognising that a one-size-fits-all approach is not feasible or preferable.

Financial authorities and FIs can choose to adopt these recommendations as appropriate and relevant, consistent with their legal and regulatory framework.

Recommendations:

1. **Establish and maintain objectives for CIR.** Financial authorities should have clearly defined objectives for incident reporting, and periodically assess and demonstrate how these objectives can be achieved in an efficient manner, both for FIs and authorities.

2. **Explore greater convergence of CIR frameworks.** Financial authorities should continue to explore ways to align their CIR regimes with other relevant authorities, on a cross-border and cross-sectoral basis, to minimise potential fragmentation and improve interoperability.

3. **Adopt common data requirements and reporting formats.** Financial authorities should individually or collectively identify common data requirements, and, where appropriate, develop or adopt standardised formats for the exchange of incident reporting information.

4. **Implement phased and incremental reporting requirements.** Financial authorities should implement incremental reporting requirements in a phased manner, balancing the authority's need for timely reporting with the affected institution's primary objective of bringing the incident under control.

5. **Select appropriate incident reporting triggers.** Financial authorities should explore the benefits and implications of a range of reporting trigger options as part of the design of their CIR regime.

6. **Calibrate initial reporting windows.** Financial authorities should consider potential outcomes associated with window design or calibration used for initial reporting.

7. **Provide sufficient details to minimise interpretation risk.** Financial authorities should promote consistent understanding and minimise interpretation risk by providing an appropriate level of detail in setting reporting thresholds, using common terminologies and supplementing CIR guidance with examples.

8. **Promote timely reporting under materiality-based triggers.** Financial authorities that use materiality thresholds should consider finetuning threshold language, or explore other suitable approaches, to encourage prompt reporting by FIs for material incidents.

9. **Review the effectiveness of CIR and cyber incident response and recovery (CIRR) processes.** Financial authorities should explore ways to review the effectiveness of FIs' CIR and CIRR processes and procedures as part of their existing supervisory or regulatory engagement.

10. **Conduct ad-hoc data collection.** Financial authorities should explore ways to complement CIR frameworks with supervisory measures as needed and engage FIs on cyber incidents, both during and outside of live incidents.

11. **Address impediments to cross-border information sharing.** Financial authorities should explore methods for collaboratively addressing legal or confidentiality challenges relating to the exchange of CIR information on a cross-border basis.

12. **Foster mutual understanding of benefits of reporting.** Financial authorities should engage regularly with FIs to raise awareness of the value and importance of incident reporting, understand possible challenges faced by FIs and identify approaches to overcome them when warranted.

13. **Provide guidance on effective CIR communication.** Financial authorities should explore ways to develop, or foster development of, toolkits and guidelines to promote effective communication practices in cyber incident reports.

14. **Maintain response capabilities which support CIR.** FIs should continuously identify and address any gaps in their cyber incident response capabilities which directly support CIR, including incident detection, assessment and training on a continuous basis.

15. **Pool knowledge to identify related cyber events and cyber incidents.** Financial authorities and FIs should collaborate to identify and implement mechanisms to proactively share event, vulnerability and incident information amongst financial sector participants to combat situational uncertainty, and pool knowledge in collective defence of the financial sector.

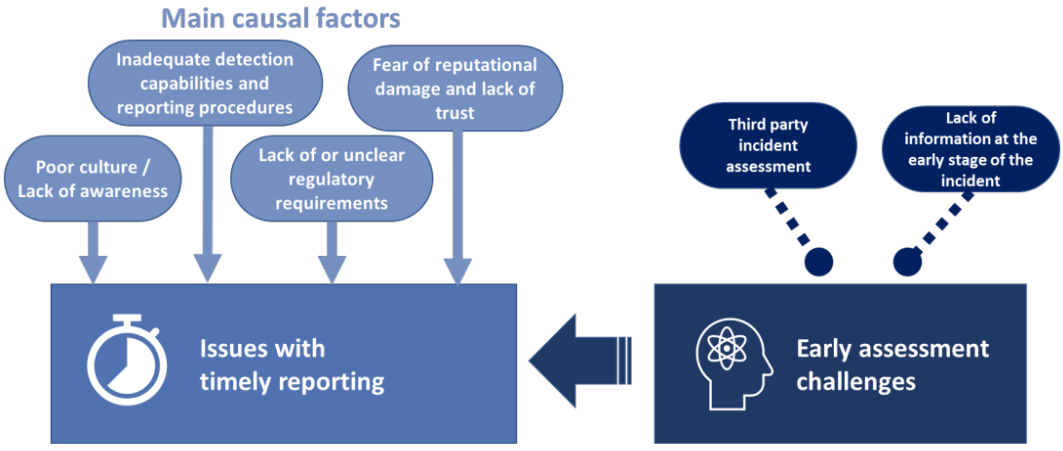
16. **Protect sensitive information.** Financial authorities should implement secure forms of incident information handling to ensure protection of sensitive information at all times.

FSB FINANCIAL STABILITY BOARD

Recommendations to Achieve Greater Convergence in Cyber Incident Reporting

Final Report

Possible causal factors to issues with timely reporting Figure 3



The report: https://www.fsb.org/wp-content/uploads/P130423-1.pdf

Cybersecurity: Protecting Investors

Commissioner Jaime Lizárraga - Remarks before the Digital Directors Network 2023 Conference

U.S. SECURITIES AND EXCHANGE COMMISSION

Good morning. Thank you, Bob [Zukis]. It is a pleasure to be here today, and I thank the Digital Directors Network for hosting this discussion about cybersecurity. This topic is so essential for the safety and resiliency of our capital markets.

My special thanks to former Commissioner Luis Aguilar for initially inviting me to speak to you today. Commissioner Aguilar had a distinguished career in public service. As the eighth longest-serving Commissioner in SEC history, he was one of only three Commissioners to have been nominated by two U.S. Presidents from different parties. A remarkable accomplishment.

It is exciting to speak to an audience of cybersecurity professionals and directors like yourselves, who share a deep commitment to robust policies and practices in cyber governance.

Since 2017, the Digital Directors Network has served as a resource to the wide variety of members it represents – that is, those responsible for designing, implementing, and testing cyber governance policies and procedures.

Over the next two days, you will hear a range of views on how best to address the complex and rapidly evolving cyber challenges that all market participants are confronting in our capital markets today.

At the SEC, we are at the forefront of addressing these challenges. In the face of rapid technological change and increased cyber threats at home and abroad, the Commission is taking action to require that market participants strengthen their cybersecurity practices.

Consistent with our congressional mandates, one of our key aims is to protect the investing public against potentially significant financial and reputational costs from cyberattacks and data breaches.

Because once victims' identities are stolen or their personal information is compromised, the damage can be irreparable and irreversible.

The Commission's actions go hand-in-hand with our ongoing efforts to modernize and update some of our outdated rules. As part of our mission

to protect investors, facilitate capital formation, and promote fair and efficient markets, we have a responsibility to update our regulatory framework to keep pace with emerging risks, whether driven by technological change or any other factor.

The Commission has proposed several rules that are designed to protect investors in our capital markets from cyber risks. These rules will require covered market entities to implement practices that will make their operations more secure and will mitigate risks to themselves, their customers, and our markets.

Why does robust cybersecurity matter? Cyberattacks and data breaches can have devastating impacts on companies and their customers and undermine investor and market confidence. In the last decade, cyberattacks of all sizes have resulted in hundreds of millions of records stolen and billions in damages to victims.

The interagency U.S. Financial Stability Oversight Counsel, or FSOC, noted in its 2021 annual report, that a major cyber incident could threaten the stability of U.S. markets in at least three ways: by

(1) disrupting a single point of failure in our financial markets, such as a key financial service provider or utility;

(2) compromising the integrity of a critical dataset; or

(3) causing a significant loss of confidence in our capital markets, resulting in market participants withdrawing from the markets.

Our capital markets are nearly $100 trillion in size – representing 40 percent of the world's total – and process over a trillion dollars of transactions per day.

By facilitating capital raising by businesses large and small, they play an instrumental role in our economy. And they serve working families who invest their savings as an optimistic way of channeling their hopes and dreams for the future – to build long-term wealth.

In light of this, it is critical that we do everything in our power to strengthen cyber practices, so that our financial markets can be more resilient and so that investors can be protected – in the most effective way possible.

The use of, and reliance on, technology in our capital markets has increased exponentially in recent years. A variety of factors have contributed to this trend. Digital innovations have led to greater interconnectedness, increased computing power and lower overall costs.

Expanded opportunities for the public to access financial services through smartphones is another factor. The COVID-19 pandemic also contributed to this digital transformation by accelerating the shift to online services to replace in-person interactions.

While these developments and innovations have the potential to increase competition, efficiency, and participation in the capital markets, they may also increase cyber risks.

Last year, the Financial Stability Board (FSB), noted in a key report that cyber incidents are "rapidly growing in frequency and sophistication," take place in the context of "growing interconnectedness of the financial system," and create greater risk of "spillover effects across borders and sectors."

To read more: https://www.sec.gov/news/speech/lizarraga-remarks-cybersecurity-051623

EIOPA and ECB call for increased uptake of climate catastrophe insurance

The European Insurance and Occupational Pensions Authority (EIOPA) and the European Central Bank (ECB) published a joint discussion paper on how to better insure households and businesses in the European Union against climate-related natural catastrophes such as floods or wildfires.

The policy options set out in the paper are aimed at boosting the uptake and efficiency of climate catastrophe insurance while creating incentives to adapt to and reduce climate risks.

“We need to increase the uptake of climate catastrophe insurance to limit the growing impact of natural disasters on the economy and the financial system,” said ECB Vice-President Luis de Guindos. “However, to reduce losses in the first place, we must ensure that a smooth and speedy green transition is complemented by effective measures to adapt to climate change.”

EIOPA Chairperson Petra Hielkema added: “Insurance plays a major role in protecting businesses and people against climate-related catastrophe losses by swiftly providing the necessary funds for reconstruction. In order to efficiently protect our society, we need to address the concern of the increasing insurance protection gap by proposing and finding appropriate solutions.”

Currently, only about one-quarter of all climate-related catastrophe losses in the European Union are insured. In some countries, the figure is below 5%. This is partly because many people underestimate the costs of climate-related damage. Some also shy away from insurance, preferring to rely on government support.

As natural disasters become both more frequent and more severe, insurance costs are expected to rise. Some insurers may reduce risk coverage or stop providing certain types of catastrophe insurance altogether, which would widen the insurance gap further.

The lack of climate catastrophe insurance can affect the economy and financial stability. If losses are not covered by insurance, the speed at which households and firms can resume their activities is reduced, slowing economic recovery.

Lasting supply chain disruptions can also lead to spillovers from one firm to another and affect firms' ability to pay back loans, thereby increasing banks' exposures to credit risk. Additionally, the financial position of governments may be weakened if they need to provide relief to cover uninsured losses.

To foster insurance coverage, EIOPA and the ECB suggest that insurers should design their policies to encourage households and firms to reduce risk, for example by granting discounts for implementing effective mitigation or adaptation measures.

To support the overall supply of insurance, the use of catastrophe bonds could be increased to pass on part of the risk to capital market investors. In the same vein, governments could set up public-private partnerships and backstops to partly cover the costs that insurers may incur in the event of major disasters.

To protect themselves and ensure that public funds are used efficiently, governments should also provide strong incentives to reduce risks.

Finally, national-level insurance schemes could be complemented by an EU-wide public scheme that makes sure sufficient funds are made available to European countries for reconstruction following rare, large-scale climate-related catastrophes.

The joint discussion paper is part of the EIOPA's sustainable finance agenda and its work to improve the overall understanding of climate-related risk. The paper aims to foster debate on how to tackle the climate insurance protection gap.

EIOPA and the ECB will collect feedback on the policy options and also discuss them in a workshop with regulators, policymakers, insurers and academics on 22 May 2023.

Policy options to reduce the climate insurance protection gap

Discussion Paper

Executive summary

Extreme weather and climate events can have significant macroeconomic implications. While the economic impact of such events in Europe has been manageable historically, it is expected to rise over time as catastrophes become more frequent and more severe due to global warming.

Catastrophe insurance is a key tool to mitigate macroeconomic losses following extreme climate-related events, as it provides prompt funding for reconstruction and should incentivise risk reduction and adaptation.

The overall societal cost of a disaster depends not only on the severity of the initial damage but also on how swiftly reconstruction can be completed. However, reconstruction can be prolonged and may even be incomplete in the absence of sufficient resources. Insurance payouts reduce uncertainty and support aggregate demand and investment for reconstruction, enabling economies to recover faster and limiting the period of lower economic output.

By contrast, without insurance, households and firms have to finance post-disaster recovery mainly with savings, credit and/or uncertain government relief, which is likely to be much less efficient.

Only about a quarter of climate-related catastrophe losses are currently insured in the EU. This insurance protection gap could widen in the medium to long term as a result of climate change, partly because repricing of insurance contracts in response to increasingly frequent and intense events may lead to such insurance becoming unaffordable.

This would further increase the burden on governments, both in terms of macroeconomic risks and in terms of fiscal spending to cover uninsured losses. This may raise government debt burdens of EU countries and increase economic divergence.

A widening insurance protection gap may also pose financial stability risks and reduce credit provision in countries with large banking sector exposures to catastrophe risk events.

This discussion paper sets out possible actions which should be considered to tackle this protection gap and mitigate catastrophe risks from climate change in the EU by means of insurance coverage and adaptation measures.

These efforts should be complementary to ambitious mitigation policies to tackle climate change and reduce associated catastrophe risks, and should not be seen as a substitute for such policies.

To read more: https://www.eiopa.europa.eu/system/files/2023-04/ecb.policyoptions_EIOPA~c0adae58b7.en_.pdf

2022 Annual Report

PCAOB
PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD

Goal One: Modernize Standards

Effective standards advance audit quality and are foundational to the PCAOB's execution of its mission to protect investors. Not only do our standards provide the requirements auditors must satisfy when conducting their audits, they also serve as the basis for our inspection and enforcement activities.

When the PCAOB was first getting off the ground in 2003, it adopted existing standards that had been set by the auditing profession on what was intended to be an interim basis.

Twenty years later, far too many of those interim standards remain unchanged. The world has changed since 2003. And our standards must adapt to keep up with developments in auditing and the capital markets.

So in 2022, the Board announced one of the most ambitious standard-setting agendas in PCAOB history, and our staff began work on more than 30 standards within 13 standard-setting and research projects.

Goal Two: Enhance Inspections

Inspecting registered public accounting firms is one of the most important tools the PCAOB uses to protect investors.

In fact, the Division of Registration and Inspections is our largest division, with over 460 dedicated professionals inspecting roughly 200 audit firms and 800 audit engagements in more than 30 jurisdictions around the world each year.

PCAOB inspections determine whether firms are complying with PCAOB standards meant to protect investors, and inspectors' work can also provide information that may lead to PCAOB investigations and enforcement actions, as well as standard setting.

The PCAOB's inspection reports provide valuable information to investors, audit committees, and others to help inform their decisions. And the inspection process is the PCAOB's principal means of evaluating the state of audit quality to best keep investors protected.

In 2022, the PCAOB also enhanced its inspections by adapting to emerging risks and issues around the world and providing new insights. Additionally,

the PCAOB is now inspecting registered firms in Mainland China and Hong Kong for the first time in PCAOB history. (See page 10 for more on the PCAOB's work to gain complete access to inspect and investigate firms in Mainland China and Hong Kong.)

Goal Three: Strengthen Enforcement

The PCAOB's enforcement program protects investors by holding accountable those who put investors at risk by violating PCAOB rules and standards and other related laws and rules. Strong enforcement and meaningful sanctions also deter wrongdoing.

In 2022, the PCAOB approached enforcement with a renewed vigilance, increasing average penalties, pursuing enforcement actions involving certain types of violations for the first time, and taking steps to identify wrongdoing proactively by expanding the use of sweeps of firms to determine whether there may be a violation of PCAOB standards or rules.

Goal Four: Improve Organizational Effectiveness

The PCAOB's most valuable resource is people, including the more than 800 dedicated professionals on our staff who carry out our mission, as well as external stakeholders whose input makes us more effective.

In 2022, the PCAOB took significant steps to invest in our staff and to enhance our stakeholder engagement.

Strategic Goals

The PCAOB's 2022-2026 strategic plan sets out four strategic goals that guide the organization's efforts to achieve its mission of protecting investors.

Protecting Investors Through One of the Most Ambitious Standard-Setting Agendas in PCAOB History

The PCAOB made progress after updating its standard-setting and research agendas in 2022. More remains to be done. As of December 31, 2022, these were the PCAOB's active research and standard-setting projects. Track and learn more about these projects at **www.pcaobus.org/standards**. *(See page 14 for more on the PCAOB's advisory groups, which in 2022 provided perspective on our standard-setting and research agendas.)*

Short-Term Standard-Setting Projects

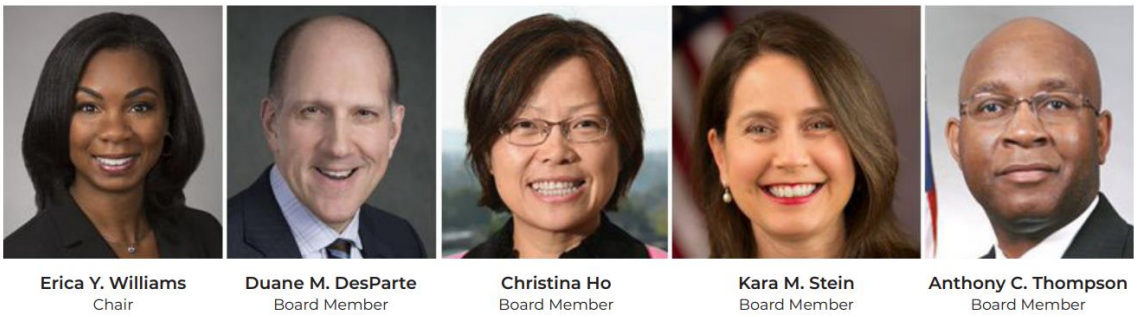
- Quality Control
- Confirmation
- Noncompliance with Laws and Regulations
- Attestation Standards Update
- Going Concern
- Interim Standards – AS 1000
- Amendments Related to Certain Aspects of Designing and Performing Audit Procedures that Involve Technology-Assisted Data Analysis

Mid-Term Standard-Setting Projects

- Substantive Analytical Procedures
- Fraud
- Interim Ethics and Independence Standards
- Interim Standards

Research Projects

- Data and Technology
- Firm and Engagement Performance Metrics



The report: https://assets.pcaobus.org/pcaob-dev/docs/default-source/about/administration/documents/annual_reports/2022-annual-report_final.pdf?sfvrsn=d73be283_2

Supercharging security with generative AI

Sunil Potti, VP/GM, Google Cloud Security

Google Cloud

At Google Cloud, we continue to invest in key technologies to progress towards our true north star on invisible security: making strong security pervasive and simple for everyone.

Our investments are based on insights from our world-class threat intelligence teams and experience helping customers respond to the most sophisticated cyberattacks.

Customers can tap into these capabilities to gain perspective and visibility on the most dangerous threat actors that no one else has.

Recent advances in artificial intelligence (AI), particularly large language models (LLMs), accelerate our ability to help the people who are responsible for keeping their organizations safe.

These new models not only give people a more natural and creative way to understand and manage security, they give people access to AI-powered expertise to go beyond what they could do alone.

At the RSA Conference 2023, we are excited to announce Google Cloud Security AI Workbench, an industry-first extensible platform powered by a specialized, security LLM, Sec-PaLM.

This new security model is fine-tuned for security use cases, incorporating our unsurpassed security intelligence such as Google's visibility into the threat landscape and Mandiant's frontline intelligence on vulnerabilities, malware, threat indicators, and behavioral threat actor profiles.

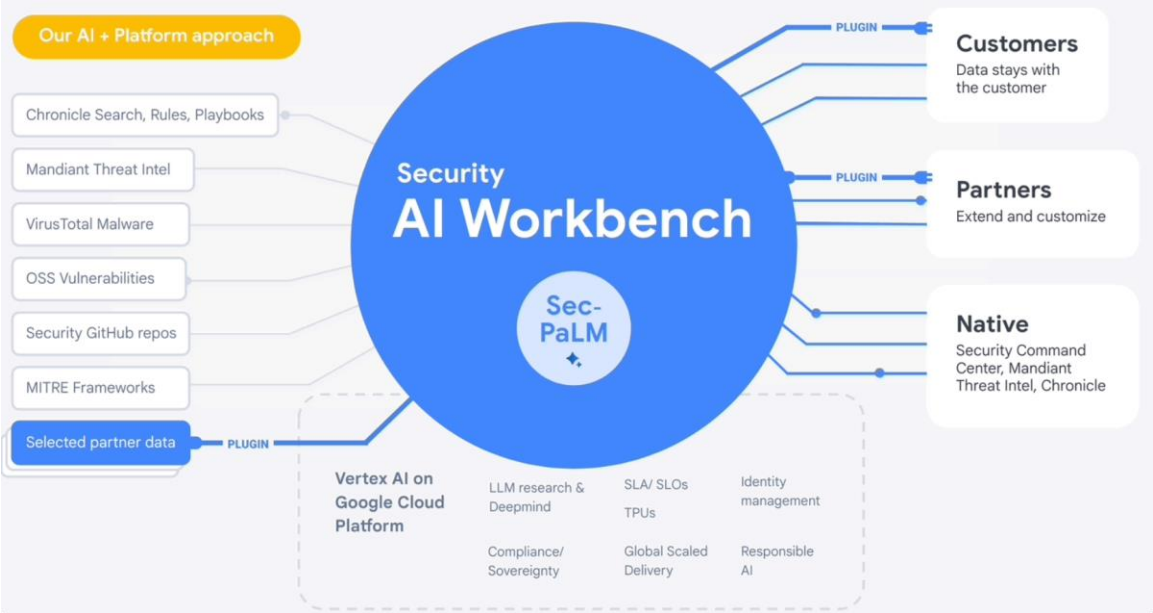
Google Cloud Security AI Workbench powers new offerings that can now uniquely address three top security challenges: threat overload, toilsome tools, and the talent gap.

It will also feature partner plug-in integrations to bring threat intelligence, workflow, and other critical security functionality to customers, with Accenture being the first partner to utilize Security AI Workbench.

The platform will also let customers make their private data available to the platform at inference time; ensuring we honor all our data privacy commitments to customers.

Because Security AI Workbench is built on Google Cloud's Vertex AI infrastructure, customers control their data with enterprise-grade

capabilities such as data isolation, data protection, sovereignty, and compliance support.



To read more: https://cloud.google.com/blog/products/identity-security/rsa-google-cloud-security-ai-workbench-generative-ai

ESAs call for vigilance in the face of mounting financial risks

The three European Supervisory Authorities (EBA, EIOPA and ESMA - ESAs) issued their Spring 2023 Joint Committee Report on risks and vulnerabilities in the EU financial system.

While noting that EU financial markets remained broadly stable despite the challenging macro environment and recent market pressure in the banking sector, the three Authorities are calling on national supervisors, financial institutions and market participants to remain vigilant in the face of mounting risks.

The second half of 2022 witnessed a worsening of the macro environment due to high inflation and tighter financial conditions, and the economic outlook remains uncertain.

Although recent growth forecasts no longer point to a deep recession and inflation is showing signs of moderation, price growth may remain elevated for longer than previously expected.

Recent market pressure on banks following the collapse of a few midsize banks in the United States and the emergency merger of the distressed Credit Suisse with the Union Bank of Switzerland (UBS) highlighted continued high market uncertainty, the sensitivity of the European financial system to exogenous shocks and potential risks related to the end of over a decade of very low interest rates.

Asset prices were highly volatile over the past months with market liquidity fragile. Sharp movements in prices triggered sizeable margin calls and put some market participants under liquidity strains, notably non-financial corporations and non-bank financial institutions.

High levels of uncertainty and imbalances in the supply and demand of liquidity are a drag on the financial system's resilience against further external shocks. In addition to these risks, geopolitical tensions, environmental threats and an increase in the frequency and sophistication of cyberattacks further complicate the risk landscape.

Against the backdrop of these risks and vulnerabilities, the Joint Committee of the ESAs advises national supervisors, financial institutions and market participants to take the following policy actions:
- financial institutions and supervisors should remain prepared for a deterioration in asset quality and supervisors should keep a close eye on loan loss provisioning;

- the broader impact of policy rate increases and sudden rises in risk premia on financial institutions and market participants should be considered and accounted for in (liquidity) risk management;

- liquidity risks arising from investments in leveraged funds and the use of interest rate derivatives should be monitored closely;

- financial institutions and supervisors should closely monitor the impacts of inflation risk. Inflation can have an impact on asset valuation and asset quality as borrower debt servicing is affected. Inflationary trends should be taken into account in product testing, product monitoring and product review phases and investors should be made aware of the effects of inflation on real returns;

- banks should pursue prudent capital distribution policies to ensure their long-term financial resilience given the uncertain medium-term outlook for profitability;

- the strong regulatory frameworks that underpin the resilience of the financial sector are to be maintained, including by faithfully implementing the finalization of Basel III in the EU without delay and with as little deviation as possible, and by avoiding further deviations from EIOPA's advice on the Solvency II review;

- risk management capabilities and disclosures for environmental, social and governance (ESG) risks should be enhanced as these risks are increasingly becoming a source of financial risk; and

- financial institutions should allocate adequate resources and skills to ensure the security of their information and communication technology (ICT) infrastructures and adequate ICT risk management.

To read more: https://www.eiopa.europa.eu/esas-call-vigilance-face-mounting-financial-risks-2023-04-25_en

EBA identifies fraud in retail payments and over indebtedness as key issues affecting consumers

The European Banking Authority (EBA) published the 8th edition of its Consumer Trends Report for 2022/23, which summarises trends observed for the products and services under the EBA's consumer protection mandate.

The Report has also identified two issues facing consumers in the EU: fraud in retail payments and over-indebtedness and arrears. These issues will shape the EBA's consumer protection priorities over the next two years.

The Report presents quantitative data for the retail banking products which covers mortgage credit, consumer credit, payment accounts, payment services, electronic money and deposits.

The Report observes that mortgage credit was affected by rising inflation and the normalisation of interest rates, while credit products were impacted by poor creditworthiness assessments and the rise of new and unregulated credit products.

All these issues have been identified as key drivers for consumers' repayment difficulties and, ultimately, over-indebtedness.

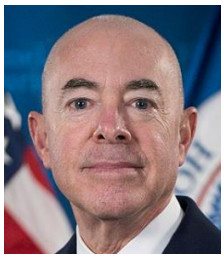
Fraud in retail payments, mainly perpetrated by new and different techniques implemented by fraudsters, was the other identified issue as experienced by consumers, based, inter alia, on fraud data collected from the year 2021 when financial institutions in several EU Member States had not complied yet with the requirements sets out in Payment Services Directive (PSD2) and the EBA's technical standards on strong customer authentication.

The Report is based on information provided by the national authorities of the 27 EU Member States, national and EU consumer associations, the members of the 'Financial Dispute Resolution Network', and EU industry associations, and quantitative data from a variety of different sources.

The report:
https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2023/1054879/Consumer%20Trends%20Report%202022-2023.pdf

2023 State of Homeland Security Remarks: Tackling an Evolving Threat Landscape – Homeland Security in 2023

Secretary Mayorkas delivered the State of Homeland Security address at the Council on Foreign Relations



Good morning, everybody. Margaret, thank you for the introduction and for the discussion we are going to have in just a few minutes. My thanks to the Council on Foreign Relations for hosting us and thanks to all of you for being here. I would like to recognize two individuals, if I may, who have special meaning to our department. Our second Secretary of Homeland Security, Michael Chertoff. And former United States Congresswoman Jane Harman.

Reflecting on the state of our homeland security in 2023, it seemed fitting to pose a fundamental question to a generative AI model: "in one sentence, describe how the homeland security threat environment has evolved over the past 20 years."

We are, after all, confronting a dramatically changed environment compared to the one we faced in March 2003. One that could change even more dramatically, as AI grips our imaginations and accelerates into our lives in uncharted and basically unmanaged fashion.

Deeply fascinated by generative AI's promise of new advances and discoveries, greatly concerned for its capacity for error and its impact on our humanity, and keenly alert to its potential for harm in the hands of an adversary, I waited only seconds for the AI model's answer:

"The homeland security threat environment has evolved from a primarily focused counterterrorism posture to a complex and diverse landscape of challenges that include cyberattacks, domestic extremism, and the COVID-19 pandemic, among others."

A straightforward answer to an important question that addresses the evolved threat landscape that our Department of Homeland Security must now confront. Its evolution is about to accelerate.

Only about six months ago, engaging with an AI chatbot was reserved for a few in Silicon Valley and universities. Today about 100 million users per

month are asking an AI chatbot just about anything, from recipe recommendations to requests for scientific analyses.

The exponential growth of internet technology and the change it has driven has been extraordinary. As we reflect on the state of our homeland security today, that explosive growth compels the question: what will this growth mean for our safety and security over the next 20 years?

We stand at the outset of what President Biden has aptly described as a "decisive decade" for our world. It is the same for our homeland security. Revolutionizing technological innovations, growing political and economic instability, widening wealth inequality, a rapidly changing climate, increasingly aggressive nation states, emerging infectious diseases, and other forces are transforming the global landscape, challenging and sometimes rendering moot a nation's borders, and bringing national and international threats to any community's doorstep.

Our Department was founded to protect us in the wake of the tragedy and devastation inflicted by the terrorist attacks of 9/11, bringing together 22 agencies from across the Federal Government charged with the mission of securing our homeland.

Back then, our country was focused on the threat of foreign terrorists who sought to enter the United States and do us harm. Over the next ten years emerged the threat of the homegrown violent extremist, the individual already resident here who was radicalized to violence by a foreign terrorist ideology.

While those threats certainly persist, today lone offenders and small cells of individuals motivated by a wide range of grievances and violent extremist ideologies – from white supremacy and anti-Semitism to anti-government attitudes – pose the most persistent and lethal terrorism-related threat in the United States.

The effects of climate change have intensified. Wildfire season is no longer confined to the summer months but is now year-round. Tornadoes and named hurricanes in the United States are more frequent and more destructive.

Just a few weeks ago in Mississippi, I surveyed the devastation wrought by a tornado that, in 20 seconds and at speeds up to 200 miles per hour, ripped through a small town, destroying multiple communities and taking the lives of more than 20 people.

Not for a century have we confronted the calamity of an infectious disease as we have over the past three years. COVID-19 took more than one million lives here in the United States, impacted every aspect of our daily life, and

forced on us a new understanding of the threat pandemic diseases can pose as they spread through paths of international trade and travel.

Globally, the impacts of disasters coupled with the rise of authoritarianism, corruption, conflict, violence, and persecution have resulted in an historic displacement and migration of people around the world and a consequent strain on immigration systems ill-equipped to address it.

According to the United Nations High Commissioner for Refugees, at the end of 2021, 89.3 million people worldwide had fled their homes due to conflict, violence, fear of persecution and human rights violations. This is the most since World War II and more than double the number of people who remained forcibly displaced a decade ago.

Criminal organizations have capitalized on this surge. The reach and growing ruthlessness of smuggling organizations have changed how people migrate. Drug trafficking organizations have grown in sophistication and power, creating new means of manufacturing and selling death and destruction.

From late 1989 through early 2001, I prosecuted federal drug trafficking crimes, from the trafficking of cocaine to methamphetamine to black tar heroin and more. Nothing I saw then matches the scourge of fentanyl that we have confronted for over the past five years. 46,802 overdose deaths in 2018; 57,834 in 2020, and 71,238 in 2021.

Over that same time, those seeking to exploit the most vulnerable have taken their depravity to an unimaginable level. The National Center for Missing and Exploited Children, the nation's clearinghouse for child sexual abuse material, received over 32 million cyber tips in 2022, corresponding to more than 88 million images and videos of child sexual abuse, a roughly 75 percent increase in the last five years.

88 million images and videos of child sexual abuse.

As threats of the past have changed in form, complexity, and magnitude, so too have new threats emerged. This is perhaps nowhere more acute than in cyberspace.

Some estimate that roughly 14.4 billion devices are connected as part of the Internet of Things, everything from our home thermostats and doorbells to our electric grid and fuel pipelines. This has brought significant advances in capabilities and conveniences, but it also has exponentially increased the ways our interconnected, digital world can be exploited to do us harm.

Today, malicious cyber actors are capable of disrupting gasoline supplies across an entire region of the country, preventing hospitals from delivering

critical care, and causing disruption in some of the school systems around our country.

Nation states like the People's Republic of China and Russia upend our rules-based international order and threaten our security at home, whether through cyberattacks, abuse of our trade and travel systems, or through disinformation campaigns that seek to undermine our democratic institutions. Our homeland security has converged with our broader national security.

The profound evolution in the homeland security threat environment, changing at a pace faster than ever before, has required our Department of Homeland Security to evolve along with it.

We have built new institutions, modernized our approach and processes, developed new capabilities, and are harnessing innovation as we deliver critical services that are more in demand than ever before.

Our overarching strategy is one of partnership. Homeland security cannot be accomplished by government alone; it requires collective action.

To meet the threat of domestic violent extremism, we created the Center for Prevention Programs and Partnerships to share with local communities the best practice models of identification and intervention when an individual is exhibiting signs of moving towards violence.

Through our grant programs we are helping communities build threat prevention capabilities where previously they did not exist, responding to the reality that major metropolitan areas are no longer our adversaries' only targets.

Across the Federal Government, we are working with communities impacted by unprecedented extreme weather events to strengthen their long-term recovery.

We have developed for the first time Department-wide incident management teams to lead all-of-government responses to emergent challenges, from vaccinating millions of Americans against COVID-19 and resettling Afghan nationals in Operation Allies Welcome, to providing protection for fleeing Ukrainians in Uniting for Ukraine.

We are coordinating and sharing intelligence with our partner nations and executing whole of government disruption and dismantlement campaigns to attack cartels.

In collaboration with diaspora communities here in the United States, we are building lawful pathways, so that migrants fleeing persecution can

access safe and orderly avenues to obtain the humanitarian relief that our laws provide.

We are working collaboratively with our partners across government, at home and abroad, and with industry and academia, to manage and reduce risk to the cyber and physical infrastructure Americans rely on every day.

We are partnering across the U.S. government to protect the most vulnerable from exploitation, whether they are migrants being trafficked by unscrupulous employers or children who are being abused online. Exploitation of the vulnerable.

In fact, yesterday we released the Third Quadrennial Homeland Security Review, our new vision for securing the homeland, and in it we included this work of combatting crimes of exploitation – such as human trafficking, child exploitation, and labor exploitation – as a dedicated homeland security mission alongside our work countering terrorism, securing our borders, administering our immigration system, securing cyberspace and critical infrastructure, and building resilience and responding to disasters. This reflects the overriding importance of supporting victims and stopping the perpetrators of these abhorrent crimes.

But, what of the threats as they could materialize tomorrow? I want to highlight new initiatives in two key areas that cut across all the Department's missions.

The People's Republic of China poses an especially grave threat to the homeland, one that indeed does touch all of our Department's missions.

Beijing has the capability and the intent to undermine our interests at home and abroad and is leveraging every instrument of its national power to do so, from its increasingly aggressive presence in the South China Sea to the overseas police stations used to harass and intimidate dissenters.

A PRC invasion of Taiwan would have profound reverberations in the homeland, putting our civilian critical infrastructure at risk of a disruptive cyberattack. We must ensure we are poised to guard against this threat today and into the future.

I have directed a 90-day Department-wide sprint to assess how the threats posed by the PRC will evolve and how we can be best positioned to guard against future manifestations of this threat:

One critical area we will assess, for example, involves the defense of our critical infrastructure against PRC or PRC-sponsored attacks designed to disrupt or degrade provision of national critical functions, sow discord and panic, and prevent mobilization of U.S. military capabilities.

Another area of assessment will involve how we can bolster our screening and vetting to identify illicit travelers from the PRC who exploit our lawful immigration and travel systems to collect intelligence, steal intellectual property, and harass dissidents, while still we must facilitate lawful travel.

Informed by engagements with subject matter experts and our stakeholders, we will take immediate action to drive down risk, lay the foundation for ongoing public-private collaboration, and work with Congress to ensure we continue to invest in these vital capabilities.

Next, and returning to where I began, we must address the many ways in which artificial intelligence will drastically alter the threat landscape and augment the arsenal of tools we possess to succeed in the face of these threats.

Our Department will lead in the responsible use of AI to secure the homeland and in defending against the malicious use of this transformational technology. As we do this, we will ensure that our use of AI is rigorously tested to avoid bias and disparate impact, and is clearly explainable to the people we serve.

I recently asked our Homeland Security Advisory Council, co-chair Jamie Gorelick is here, to study the intersection of AI and homeland security and deliver findings that will help guide our use of it and defense against it. The rapid pace of technological change – the pivotal moment we are now in – requires that we also act today.

To that end, I am directing the creation of our Department's first Artificial Intelligence Task Force that will drive specific applications of AI to advance our critical homeland security missions. The Task Force will, for example:

Integrate AI into our efforts to enhance the integrity of our supply chains and the broader trade environment. We will seek to deploy AI to more ably screen cargo, identify the importation of goods produced with forced labor, and manage risk.

The Task Force will also, among other charged, leverage AI to counter the flow of fentanyl into the United States.

We will explore using this technology to better detect fentanyl shipments, identify and interdict the flow of precursor chemicals around the world, and target for disruption key nodes in the criminal networks.

Countering the multi-faceted threat posed by the PRC, learning from major cyber incidents, and harnessing the power of AI to advance our security will draw on the entirety of the capabilities and expertise the 260,000 personnel of DHS bring to bear every single day.

It will require continued investment in our operational cohesion, our ability to work together in ways our founders never imagined.

We must never allow ourselves to be susceptible to 'failures of imagination,' which, as the 9/11 Commission concluded nearly 20 years ago, held us back from connecting the dots and preparing for the destruction that was being planned on that tragic day.

We must instead look to the future and imagine the otherwise unimaginable, to ensure that whatever threats we face, our Department – our country – will be positioned to meet the moment.

It is an especially challenging imperative to fulfill at a time not only of rapid change, but also of acute political divisiveness; when issues of homeland security that traditionally were unifying no longer are so, and when our adversaries continue to exploit innovations designed to bring us closer together, like social media, to push us apart.

We must imagine a world where even more potent and lethal synthetic opioids or infectious diseases plague our communities. Where an earthquake or catastrophic storm intensifies already historic levels of migration in our hemisphere.

Where criminals 3D print weapons or modify consumer technologies like drones to evade law enforcement. Where cyber criminals are emboldened to the point of holding for ransom the critical services of an entire city.

At the Department of Homeland Security, we have the tools and talent to meet the moment today. We are taking the actions and making the investments to ensure we will continue to adapt and meet the moment into the future. We are more fit for purpose than at any time in our 20-year history.

This is a collective effort: we must all come together in the service of our homeland security. We must call upon our collective imagination, our commitment to a better future, and our fundamental love of country that binds us together, to protect our homeland.

Thank you.

To read more: https://www.dhs.gov/news/2023/04/21/2023-state-homeland-security-remarks-tackling-evolving-threat-landscape-homeland

Statistical release: BIS international banking statistics and global liquidity indicators at end-December 2022

Key takeaways

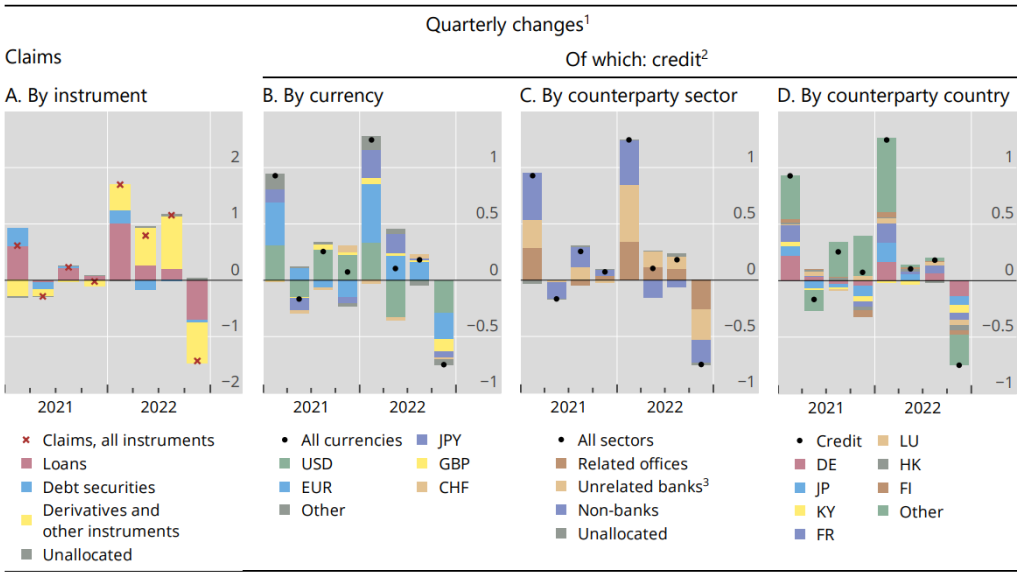
- Banks' cross-border claims fell by $1.4 trillion in Q4 2022, slowing the year-on-year (yoy) growth rate to 6%. Both lower bank credit (ie loans and holdings of debt securities) and a drop in the market value of banks' derivatives and other residual instruments contributed to the decline.

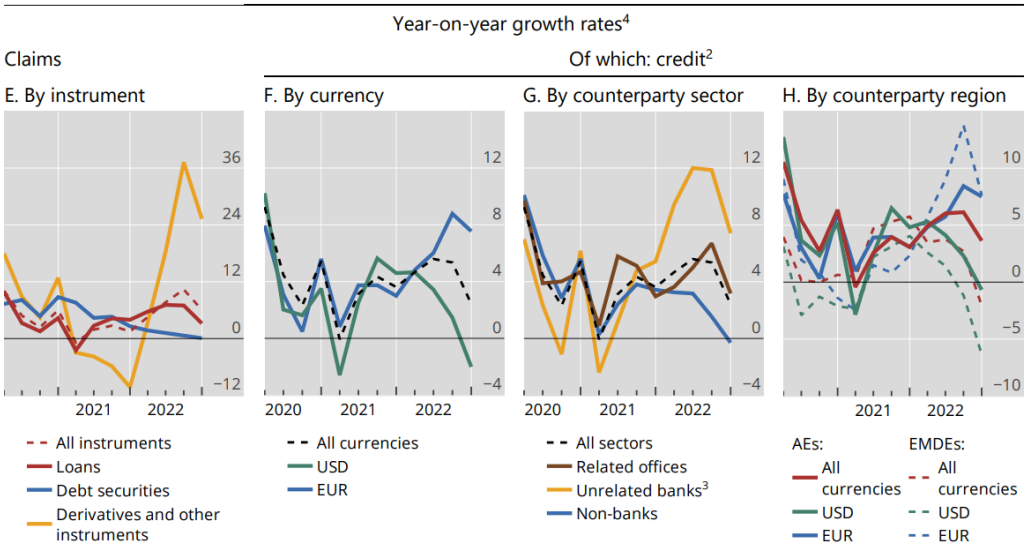
- Global cross-border bank credit (ie loans and holdings of debt securities) fell by $749 billion, or $400 billion on a seasonally adjusted basis. Euro-denominated credit declined by $231 billion after expanding earlier in the year.

- Cross-border bank credit to emerging market and developing economies (EMDEs) fell by $179 billion in Q4 2022 due to weaker dollar lending. Credit to the Asia-Pacific region contracted the most.

- The BIS global liquidity indicators (GLIs) show a large contraction in dollar credit to non-banks in EMDEs in Q4 2022. Dollar credit to EMDEs shrank by 4%, a rate last seen during the Great Financial Crisis of 2007–09.

Changes in banks' global cross-border claims — Graph 1





[1] Quarterly changes adjusted for breaks in series and exchange rate fluctuations, in trillions of US dollars. [2] Credit refers to loans and holdings of debt securities, ie excluding from "claims" all other instruments (derivatives with positive market value, equity and other residual instruments). [3] Includes credit to central banks and to banks unallocated by subsector. [4] Annual compound adjusted change, in per cent.

Source: BIS locational banking statistics.

Global cross-border credit dropped in late 2022

The BIS locational banking statistics (LBS) show that banks' cross-border claims fell by $1.4 trillion during the fourth quarter of 2022 (Graph 1.A).

This decline slowed yoy growth to 6% on an FX- and break-adjusted basis (Graph 1.E).

Graph 1 summarises the changes (top row) and the annual growth rates (bottom row) across instruments, currencies and counterparties.

The contraction in Q4 2022 reflected both a drop in the gross positive market value of derivatives and other instruments (–$718 billion, Graph 1.A, yellow bars) and a decrease in credit (–$749 billion).

Seasonal factors, eg the tendency for claims to contract at year end, accounted for roughly half of the overall decline in Q4.

The weakness in cross-border bank credit was evident across all major currencies (Graph 1.B).

In Q4, US dollar-denominated credit fell by $293 billion to $14.6 trillion, 2% lower than at end-2021 (Graph 1.F).

Euro-denominated credit, which had grown in the previous three quarters, dropped by $231 billion, the largest decline since end2019.

Even so, at $8.9 trillion, euro credit at end-2022 was 8% higher than at end2021 (Graph 1.F), due to brisk growth in cross-border lending within the euro area.

Sterling credit fell sharply (–$106 billion) against the backdrop of gilt market dysfunction in September-October 2022.

Cross-border credit to all sectors declined, with interbank positions contracting the most (Graphs 1.C and 1.G).

Interbank credit shrank by $533 billion, although more than half of this reflects seasonality in the data.

Interbank credit to unrelated banks and to related offices dropped by more than $250 billion each. Credit to non-banks fell by $199 billion, bringing the yoy growth rate to –0.3%.

To read more: https://www.bis.org/statistics/rppb2304.pdf

Tow Truck Taxonomies: Remarks before Eurofi

Commissioner Hester M. Peirce, U.S. Securities and Exchange Commission

Thank you for the chance to address you this morning. I particularly appreciate your welcoming me to address environmental, social, and governance ("ESG") issues despite my heterodox – some might say heretical – views. You will be happy to know, therefore, that I speak only for myself, and not necessarily for the US Securities and Exchange Commission ("SEC") or my fellow commissioners.

Let me state those views briefly.

First, I am concerned that ESG standards, intentionally or not, drive private capital to uses that check the right officially sanctioned ESG box, not where it will best meet human needs and solve societal problems.

Second, ESG rulemaking, by concentrating capital in favored assets, could become a source of systemic instability.

The third concern, which exacerbates the first two, is the considerable international pressure to converge on a single set of ESG standards. If every jurisdiction directs capital using a single set of standards, poor choices will reverberate through the global economy.

ESG is an ambiguous term, the depths of which I do not have time to plumb. Companies, asset managers, and investors always have considered a wide range of factors in deciding how to spend or invest their money. Some of those factors might today get an ESG label, but we do not need ESG-specific standards to serve investors' needs; materiality-based disclosure standards already do this.

Today's ESG-specific standards too often have a different purpose. These standards cannot help but direct the allocation of private capital, especially when they are combined with sustainable finance initiatives designed to encourage financing of favored activities and the defunding of disfavored activities. Indeed, they appear intended to do exactly this: to direct private capital flows. As such, they are meant not primarily to serve investors' needs but rather to direct the allocation of private capital to further government ends.

This objective, and not concerns about consistency or comparability, is what distinguishes voluntary ESG standards, which have been around for many years, from the mandatory standards that we are increasingly rushing to adopt.

The parallel, though not identical, standards the United States, the European Union, and the International Sustainability Standards Board ("ISSB") are developing are more ambitious, complicated, and costly than anything we have seen before in the corporate reporting realm.

This commandeering of private capital in the name of ESG causes me grave concerns. To illustrate why I think this sustainability-themed centralized allocation of capital is a bad development, let me tell you a story.

Several months ago, I found myself waiting for a long time by the side of the road for a tow truck. A first tow truck arrived relatively early in the evening, but the driver, mumbling that "This job is impossible!" drove off after looking at the car's severely damaged wheel.

Many hours later, after a dark chill had set in, a second truck arrived. This driver pulled up, got out, and quickly and without saying much, assessed the situation. He then calmly set to work by the light of his cellphone.

With remarkable skill, alacrity, and precision, he removed the wheel of the car, inspected the considerable extent of the damage, provided an estimate for its repair, lifted the car, and gradually and methodically worked it onto the back of his truck. He was an expert doing a difficult job in uncomfortable circumstances with confidence, meticulousness, and ease.

After about fifteen minutes, he was on his way with the car in tow. The driver's skill, deep knowledge of his craft – a knowledge that involved so many disciplines such as math, physics, mechanical skill, technical ability, a bit of psychology, and spatial relations – is a miracle that repeats itself billions of times each day; each person possesses a unique set of talents, interests, skills, and experiences.

Why am I going on about tow-truck drivers? That incident helped me to put my finger on my concerns around current ESG standard-setting efforts. First, that encounter renewed my appreciation for the depth and diversity of human activity and correspondingly underscored the futility of the technocratic effort to use elaborate ESG disclosure standards and taxonomies to classify the full range of human economic activity in an effort to reroute capital to human activities that we regulators favor.

It may sound like I am exaggerating the scope required to make these disclosure standards work, but let us be clear about this: This effort – if undertaken to starve unsustainable activities of capital and flood

sustainable activities with capital – necessarily entails understanding and classifying all of economic activity in terms of its effect on an increasing number of complex, sometimes mutually contradictory, metrics.

This task is impossible. Even brilliant people in tidy conference rooms far removed from the nitty-gritty complexity of the world (or these days behind screens in their cozy living rooms) cannot accurately label swathes of human activity as categorically positive or negative.

Collecting bushels of data to measure the unmeasurable and quantify the unquantifiable is an unreliable basis for deciding where to send capital, even if all these data create the illusion that we understand the world and how humans live and work in it.

As little as standard setters can hope to know about the world as it currently exists, the future remains an even greater enigma. Yes, scientists can help regulators estimate how the climate is changing, technologists can help regulators predict which solutions for mitigating and adapting to these changes look most promising, and economists can advise about the viability of those solutions.

But nobody – not even the most capable regulators advised by the most qualified experts – can prophesy where, when, and how the most important innovations will arise. A regulator trying today to drive capital flows toward green technologies might be doing the opposite inadvertently.

Solutions to our greatest problems will come – in ways we could never have imagined – from people, many of whom are just now being born and educated. In a fully taxonomized world would these people with truly original ideas be able to access capital? Inflexible taxonomies, updated through the slow political process, are static solutions to dynamic problems like food insecurity, water shortages, educational needs, air pollution, access to medical care, climate change, and many other problems we have not yet seen.

A principles-based regulatory framework designed to elicit financially material information about companies will not guarantee that these innovators are funded, but it will not foreclose their access to capital by prejudging the who, what, where, and when of innovation.
Second, ESG taxonomies, built on misplaced confidence in how accurately they capture reality, and the sustainable finance behemoth resting on top of these taxonomies will concentrate capital in ways that could create systemic instability.

Past financial crises have taught us that regulatory inducements to invest in particular sectors or in particular ways can harm investors, financial institutions, the financial system, and the broader economy.

Leading up to the great financial crisis, for example, policies designed to favor certain asset classes injected dangerous instability into the financial system. As unique as each person is, humans nevertheless sometimes behave like sheep and follow others uncritically into investing fads. Government regulation can exacerbate these trends by distorting incentives.

Moving capital to government-designated sustainable activities could create a green bubble within the financial system as investors pour money uncritically into green assets, as defined in the relevant taxonomy. We already see tell-tale signs of a problem: investors are complaining about the lack of investable assets, and, as we have seen many times before, the search for investable assets may cause them to forgo standard risk management precautions.

Asset bubbles always pop, no matter how noble the intentions of those who established the incentives that helped create them. We have no reason to expect that the distorted incentives created by ESG disclosure standards and related policies will produce a different result. And because the herding that created the bubble also likely will lead to the underfunding of activities that could produce real change but that do not fit within our taxonomies, the messy economic aftermath may not even be softened by the consolation that these standards brought us closer to solutions to any of the problems these taxonomies were designed to address.

We could mitigate the risk created by fallible regulators and herd-prone investors by allowing for diversity across jurisdictions. But increasing calls for regulatory convergence threaten diversity in ESG standards, which brings me to my third concern. While I appreciate the difficulty companies and investors face with multiple competing standards, we need to be more specific about what we mean by convergence.

If convergence allows for mutual recognition of different approaches – including a US approach to ESG disclosures truly rooted in financial materiality – then it would be a positive development. For example, the world has managed to operate with multiple sets of accounting standards. If, by contrast, convergence means that every jurisdiction has to implement substantially identical standards, then convergence raises several serious concerns.

First, if all jurisdictions use the same standard, the distortion of private capital flows will be more pronounced. Any problems in the taxonomy – favoring harmful activities or disfavoring socially useful activities – will reverberate through the whole world, rather than being confined to a particular jurisdiction.

Second, and related, if my systemic concerns are well-founded, a consistent set of ESG standards could exacerbate them by creating a global asset bubble.

Third, as the tow-truck driver reminds us, regulators will have a difficult time writing standards that apply equally well everywhere. Global standards could miss important nuances about the physical, legal, social, and cultural environment in which an activity occurs.

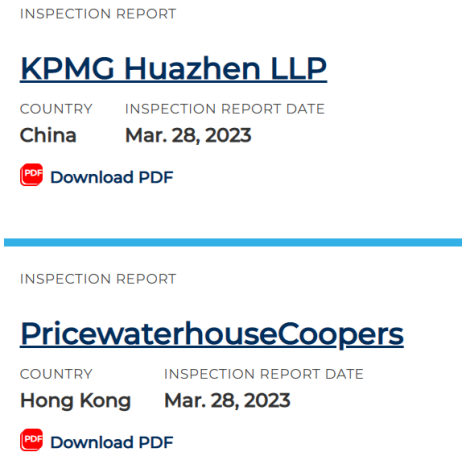
Finally, achieving convergence by applying standards extraterritorially, would undermine national sovereignty and the rule of law. A jurisdiction that has a set of procedures for adopting new disclosure standards cannot simply delegate the task to a supra-national body, such as the ISSB, or another jurisdiction, such as the EU.

To read more: https://www.sec.gov/news/speech/peirce-remarks-eurofi-042823

PCAOB Releases 2022 Inspection Reports for Mainland China, Hong Kong Audit Firms

Chair Williams says reports are "a powerful first step toward accountability," as demand for complete access continues

Public Company Accounting Oversight Board (PCAOB) Chair Erica Y. Williams made the following statement today after the PCAOB released inspection reports for two firms inspected in 2022: KPMG Huazhen LLP in mainland China and PricewaterhouseCoopers in Hong Kong.



From Chair Williams:

Thanks to the leadership of the U.S. Congress in passing the Holding Foreign Companies Accountable Act (HFCAA), last year, the PCAOB secured complete access to inspect registered public accounting firms headquartered in mainland China and Hong Kong for the first time in history.

Today, the PCAOB is releasing the inspection reports for both firms inspected in 2022: KPMG Huazhen LLP in mainland China and PricewaterhouseCoopers in Hong Kong.

Both reports show unacceptable rates of Part I.A deficiencies, which are deficiencies of such significance that PCAOB staff believe the audit firm failed to obtain sufficient appropriate audit evidence to support its work on the public company's financial statements or internal control over financial reporting.

The PCAOB inspected a total of eight engagements in 2022 – four at each of the two firms – including the types of engagements to which People's

Republic of China (PRC) authorities had previously denied access, such as large state-owned enterprises and issuers in sensitive industries.

PCAOB inspectors found Part I.A deficiencies in 100% (four of four) of the audit engagements reviewed at KPMG Huazhen and 75% (three of four) of the audit engagements reviewed for PwC Hong Kong.

As I have said before, any deficiencies are unacceptable. At the same time, it is not unexpected to find such high rates of deficiencies in jurisdictions that are being inspected for the first time. And the deficiencies identified by PCAOB staff at the firms in mainland China and Hong Kong are consistent with the types and number of findings the PCAOB has encountered in other first-time inspections around the world.

The fact that our inspectors found these deficiencies is a sign that the HFCAA was effective and the inspection process worked as it is supposed to. We identified problems so now we can begin the work of holding firms accountable to fix them.

Today's reports are a powerful first step toward accountability. By shining a light on deficiencies, our inspection reports provide investors, audit committees, and potential clients with important information so they can make informed decisions and hold firms accountable. And the power of transparency applies public pressure for firms to improve.

The remediation process is another tool we use to hold firms accountable for fixing deficiencies. By law, public inspection reports do not initially include quality control deficiencies that inspectors find. Instead, firms have one year to remediate those deficiencies. If they don't remediate those deficiencies to the Board's satisfaction, we make them public.

Finally, where appropriate, our inspectors will refer inspection findings to our enforcement team for possible action. If violations are found, our enforcement staff will not hesitate to recommend sanctions, including imposing significant money penalties and barring bad actors from performing future audits.

Last year was only the beginning of our work to inspect and investigate firms in mainland China and Hong Kong.

Our enforcement teams continue to pursue investigations, and inspectors have begun fieldwork for 2023's inspections. We anticipate fieldwork will continue off and on throughout most of the year, which is common practice for inspections such as these in jurisdictions around the world.

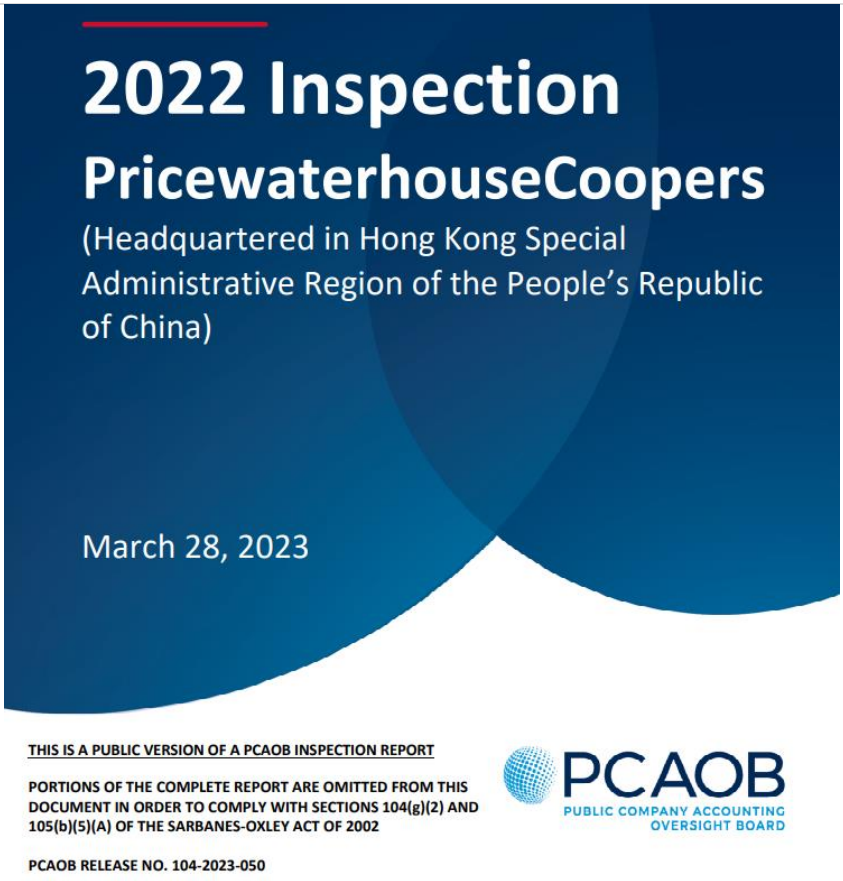
The two firms we inspected in 2022 audited 40% of the total market share of U.S.-listed companies audited by Hong Kong and mainland China firms,

and we are on track to hit 99% of the total market share by the end of this year. So, there is no question that the PCAOB is prioritizing inspections that are the most relevant to investors on U.S. markets – because protecting investors is what this is all about.

Indeed, the release of today's reports is yet another sign that investors are more protected because of Congress' leadership in passing the HFCAA. And last year's legislation, which shortened the timeline from three years to two years, provided important leverage as the PCAOB continues demanding complete access to inspect and investigate firms headquartered in mainland China and Hong Kong – with no loopholes and no exceptions.

As I have said before, should PRC authorities obstruct or otherwise fail to facilitate the PCAOB's access – in any way and at any time – the Board will act immediately to consider the need to issue a new determination.

I want to thank the hardworking inspectors, investigators, and PCAOB staff who continue this important work on behalf of investors every day.



To read more: https://pcaobus.org/news-events/news-releases/news-release-detail/pcaob-releases-2022-inspection-reports-for-mainland-china-hong-kong-audit-firms

https://pcaobus.org/oversight/inspections/firm-inspection-reports

Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

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 (if you need specific advice, you should always consult a suitably qualified professional);

- is in no way constitutive of an interpretative document;

- 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.

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.

International Association of Potential, New and Sitting Members of the Board of Directors (IAMBD)

The IAMBD offers standard, premium and lifetime membership, networking, training, certification programs, a monthly newsletter with alerts and updates, and services we can use.

The association develops and maintains three certification programs and many specialized tailor-made training programs for directors.

Join us. Read our monthly newsletter with news, alerts, challenges and opportunities. Get certified. Provide independent evidence that you are an expert.

You can explore what we offer to our members:

1. Membership - Become a premium or lifetime member.
You may visit:
https://www.iambd.org/HowToBecomeMember.html

2. Monthly Updates – Visit the Reading Room of the association at:
https://www.iambd.org/Reading_Room.htm

3. Training and Certification - Become a Certified Member of the Board of Directors (CMBD), Certified Member of the Risk Committee of the Board of Directors (CMRBD) or Certified Member of the Corporate Sustainability Committee of the Board of Directors (CMCSCBD).

You may visit:
https://www.iambd.org/Distance_Learning_and_Certification.htm

For instructor-led training, you may contact us. We can tailor all programs to meet specific requirements.