International Association of Risk and Compliance Professionals (IARCP)
1200 G Street NW Suite 800, Washington DC, 20005-6705 USA
Tel: 202-449-9750, Web: www.risk-compliance-association.com

Monday, April 25, 2022

Top 10 risk and compliance related news stories and world events that (for better or for worse) shaped the week's agenda, and what is next

Dear members and friends,

Concentration risk in crypto trading is becoming a major regulatory concern. In February, I read an interesting paper from the Financial Stability Board (FSB), with title: "Assessment of Risks to Financial Stability from Crypto-assets". We read:

"Moreover, a relatively small number of crypto-asset trading platforms that aggregate multiple types of services and activities, including lending and custody, account for the majority of crypto-assets traded. Some of these platforms operate outside of a jurisdiction's regulatory perimeter or are not in compliance with applicable laws and regulations. This presents the potential for *concentration of risks,* as well as underscores the lack of transparency on their activities."

Gary Gensler has just discussed *concentration risk* (at the Penn Law Capital Markets Association Annual Conference). We read:

"The crypto market is highly concentrated, with the bulk of trading taking place on only a handful of platforms. Amongst crypto-only exchanges, the top five platforms make up 99 percent of all trading, and just two platforms make up 80 percent of trading."

Concentration risk is a very special risk that requires special attention by supervisors, as it can jeopardise the survival of institutions. It is one of the main causes of major losses in credit institutions. Events during the 2008-2009 financial crisis have brought to light many examples.

In the Basel framework, concentration risk is one of the specific risks required to be assessed as part of the Pillar 2 framework. It refers not only to risk related to credit granted to individuals or interrelated borrowers, but to any other significant interrelated asset or liability exposures which, in cases of distress in some markets/ sectors/ countries or areas of activity, may threaten the soundness of an institution.

Chair Gary Gensler covered many other important aspects of crypto trading. I like the way he started his presentation:

"Today, you've invited me to talk about the roughly $2 trillion crypto markets.

In February, you all might have noticed Super Bowl ads for several crypto platforms. This wasn't the first time we'd seen some new innovations getting air time on the biggest TV event of the year.

Seeing these ads reminded me that, in the lead-up to the financial crisis, subprime lender AmeriQuest advertised in the Super Bowl. It went defunct in 2007. A few years before that, according to Axios, "Fourteen dotcom companies advertised during the 2000 Super Bowl, most of which are now defunct."

I know many in the audience may just have been young children at the time, but the internet was relatively new back in 2000. The dot-com bubble burst, though, created significant tremors in our markets.

Ads, thus, don't equal credibility. In crypto, there is lots of innovation, but plenty of hype. As in other start-up fields, many projects likely could fail. That's simply part of the entrepreneurial spirit in the U.S.

The SEC's remit is overseeing the capital markets and our three-part mission: protecting investors, facilitating capital formation, and maintaining fair, orderly, and efficient markets. Within the policy perimeter, regulators also care about guarding against illicit activity, a role

that is so important to us and our partners at the Department of the Treasury and the Department of Justice; and about financial stability, which is important to all financial regulators.

There's no reason to treat the crypto market differently just because different technology is used. We should be technology-neutral."

This is a very interesting presentation. Chair Gary Gensler asked one of the most important questions:

"You might wonder: how might a crypto token be a security?

The Supreme Court's 1946 Howey Test, which was about orange groves, says that an investment contract exists when there is the investment of money in a common enterprise with a reasonable expectation of profits to be derived from the efforts of others.

My predecessor Jay Clayton said it, and I will reiterate it:

Without prejudging any one token, most crypto tokens are investment contracts under the Howey Test.

Even before the Howey test, in the first several years of our federal securities laws, some entrepreneurs were notified that they had to register their offerings of chinchillas, whiskey warehouse receipts, oyster beds, and live silver foxes as securities offerings, as "the purported sale of the…property was merely camouflage and not the substance of the transaction."

Today, many entrepreneurs are raising money from the public by selling crypto tokens, with the expectation that the managers will build an ecosystem where the token is useful and which will draw more users to the project.

Thus, it is important that we work to get crypto tokens that are securities to be registered with the SEC.

Issuers of crypto tokens that are securities must register their offers and sales of these assets with the SEC and comply with our disclosure requirements, or meet an exemption.

Issuers of all kinds across a variety of markets successfully register and provide disclosures every day.

If there are, in fact, forms or disclosure with which crypto assets truly cannot comply, our staff is here to discuss and evaluate those concerns. Any token that is a security must play by the same market integrity rulebook as other securities under our laws."

Read more at Number 2 below. Welcome to the Top 10 list.

Best regards,

George Lekatis
President of the IARCP
1200 G Street NW Suite 800,
Washington DC 20005, USA
Tel: (202) 449-9750
Email: lekatis@risk-compliance-association.com
Web: www.risk-compliance-association.com
HQ: 1220 N. Market Street Suite 804,
Wilmington DE 19801, USA
Tel: (302) 342-8828

Number 1 (Page 7)

FSB Statement Welcoming Smooth Transition Away from LIBOR

Number 2 (Page 10)

Prepared Remarks of Gary Gensler On Crypto Markets

SEC Chair Gary Gensler, Penn Law Capital Markets Association Annual Conference

Number 3 (Page 17)

Central bank digital currencies: a new tool in the financial inclusion toolkit?

FSI Insights No 41, by Raphael Auer, Holti Banka, Nana Yaa Boakye-Adjei, Ahmed Faragallah, Jon Frost, Harish Natarajan and Jermy Prenio

Number 4 (Page 20)

COSTS AND PAST PERFORMANCE REPORT – 2022

Number 5 (Page 22)

PCAOB Requests Comment on Impact of Auditing Requirements Related to Estimates and Specialists

Comments Due June 10, 2022

Number 6 (Page 25)

Cybersecurity Market Analysis in support of Informed Cybersecurity Business Decisions

Number 7 (Page 28)

ENISA Cybersecurity Market Analysis Framework (ECSMAF)

Number 8 (Page 32)

Environmental, Social and Governance (ESG) risks

EBA publishes binding standards on Pillar 3 disclosures on ESG risks

Number 9 (Page 35)

Balancing on the net-zero tightrope

Sarah Breeden, Executive Director for Financial Stability Strategy and Risk and a member of the Financial Policy Committee (FPC) in UK.

Number 10 (Page 42)

Hounding scammers with litigation

lbert Shin, Manager, CyberCrime Investigation Group
Mike Trinh, Senior Counsel

Number 1

FSB Statement Welcoming Smooth Transition Away from LIBOR

Following years of preparation, the end of 2021 marked a major milestone in the transition away from LIBOR and the FSB welcomes the smooth transition to robust alternative rates across global markets, primarily overnight risk-free or nearly risk-free rates (RFRs).

The absence of any significant market disruptions is a testament to the magnitude of market participants' efforts and the level of attention from the regulators and industry bodies to support the transition to RFRs.

Stocktake of end-2021 transition

All GBP, EUR, CHF, and JPY LIBOR panels, as well as the 1-week and 2-month USD LIBOR settings, ceased as of end-2021.

The 1-, 3- and 6-month GBP and JPY LIBOR settings are being published temporarily on a synthetic basis to support legacy contracts.

While key panel-based USD LIBOR settings will continue until end-June 2023, this is intended to support the run-off of a substantial proportion of legacy contracts.

US Banking Supervisors as well as many other authorities in FSB jurisdictions have strongly encouraged firms to cease new use of USD LIBOR after end-2021, subject only to some limited exceptional use to support an orderly transition.

It is important to continue to build market liquidity of products referencing robust RFRs and to use SOFR across global markets.

The transition in GBP, EUR, CHF, and JPY LIBOR shows that RFRs can be used successfully in a wide variety of markets including bonds, derivatives and lending markets.

There has already been a significant and smooth transition away from USD LIBOR for many markets.

New activity in USD over-the-counter derivatives and capital markets products is predominantly linked to SOFR now.

Additionally, the transition from USD LIBOR to SOFR appears to be progressing smoothly in lending markets.

Use of SOFR has increased in exchange traded derivatives, however greater progress will need to be achieved in certain markets, such as in Eurodollar futures and options markets, where significant LIBOR-linked activity remains.

Key messages for 2022-23

Given the significant use of USD LIBOR globally, the FSB emphasises that firms must have plans in place to ensure their preparedness for the cessation of the USD LIBOR panel.

The FSB continues to support a smooth transition of legacy LIBOR contracts as part of a wider market transition to robust RFRs that will not reintroduce the vulnerabilities experienced with LIBOR.

The FSB again highlights the Statement on Credit Sensitive Rates by the Board of the International Organization of Securities Commissions (IOSCO).

Firms should have already ceased new use of USD LIBOR. It has been repeatedly emphasised by authorities that the continuation of some USD LIBOR settings through to end-June 2023 is intended only to allow legacy contracts to mature.

In addition, it affords market participants more time to take the necessary steps for the conversion of legacy contracts.

Between now and end-June 2023, firms with USD LIBOR exposures should take the steps set out in the FSB's Global Transition Roadmap.

To ensure financial stability, it is important that market participants transition from LIBOR and other IBORs that are set to be discontinued.

The FSB continues to encourage adoption of overnight RFRs and active transition away from USD LIBOR before June 30, 2023 where appropriate.

The FSB recognises that in some cases there may be a role for RFR-derived term rates and has set out the circumstances where the limited use of RFR-based term rates would be compatible with financial stability.

The FSB also continues to support engagement with emerging markets and developing economies (EMDEs) to maintain a smooth transition from LIBOR to RFRs, across all global markets.

The FSB encourages firms to maintain momentum in active transition of legacy LIBOR contracts that reference synthetic GBP and JPY LIBOR settings.

The FCA has been clear that synthetic LIBOR is a temporary bridging solution to allow more time for legacy contracts to transition to robust RFRs. Synthetic LIBOR rates cannot be guaranteed beyond end-2022. For JPY LIBOR, the FCA's intention is that it will cease at end-2022.

The FCA has announced that, during the course of 2022, it will seek views on retiring 1-month and 6-month synthetic sterling LIBOR at the end of 2022, and on when to retire 3-month sterling synthetic LIBOR. It should be noted that active transition remains the best way for parties to retain control and certainty over their contractual terms.

The FSB plans to conduct a follow-up assessment in H2 2022 to identify any remaining transition and supervisory challenges to support LIBOR transition effort.

Number 2

Prepared Remarks of Gary Gensler On Crypto Markets

SEC Chair Gary Gensler, Penn Law Capital Markets Association Annual Conference

Thank you. It's great to be with you all at this event, particularly as the University of Pennsylvania is my alma mater. I was over at Wharton, and what I knew of the law school is that the library stacks were a great place to study. It was so quiet there, though I don't know if that's still the case.

As is customary, I'd like to note that my views are my own, and I'm not speaking on behalf of the Commission or SEC staff.

Today, you've invited me to talk about the roughly $2 trillion crypto markets.

In February, you all might have noticed Super Bowl ads for several crypto platforms. This wasn't the first time we'd seen some new innovations getting air time on the biggest TV event of the year.

Seeing these ads reminded me that, in the lead-up to the financial crisis, subprime lender AmeriQuest advertised in the Super Bowl. It went defunct in 2007. A few years before that, according to Axios, "Fourteen dotcom companies advertised during the 2000 Super Bowl, most of which are now defunct."

I know many in the audience may just have been young children at the time, but the internet was relatively new back in 2000. The dot-com bubble burst, though, created significant tremors in our markets.

Ads, thus, don't equal credibility. In crypto, there is lots of innovation, but plenty of hype. As in other start-up fields, many projects likely could fail. That's simply part of the entrepreneurial spirit in the U.S.

The SEC's remit is overseeing the capital markets and our three-part mission: protecting investors, facilitating capital formation, and maintaining fair, orderly, and efficient markets.

Within the policy perimeter, regulators also care about guarding against illicit activity, a role that is so important to us and our partners at the Department of the Treasury and the Department of Justice; and about financial stability, which is important to all financial regulators.

There's no reason to treat the crypto market differently just because different technology is used. We should be technology-neutral.

So I'd like to mention three areas related to the SEC's work in this area: platforms, stablecoins, and crypto tokens.

Platforms

First are the crypto trading and lending platforms, whether they call themselves centralized or decentralized (DeFi).

These platforms have scale, recently trading crypto worth more than $100 billion a day.

The crypto market is highly concentrated, with the bulk of trading taking place on only a handful of platforms. Amongst crypto-only exchanges, the top five platforms make up 99 percent of all trading, and just two platforms make up 80 percent of trading.

In crypto-to-fiat transactions, 80 percent of trading is on five trading platforms.

Similarly, the top five DeFi platforms account for nearly 80 percent of trading on those platforms.

Furthermore, these platforms likely are trading securities. A typical trading platform has dozens of tokens on it, at least. In fact, many have well in excess of 100 tokens. As I'll address later, many of the tokens trading on these platforms may well meet the definition of "securities."

While each token's legal status depends on its own facts and circumstances, given the Commission's experience with various tokens that are securities, and with so many tokens trading, the probability is quite remote that any given platform has zero securities.

Thus, I've asked staff to work on a number of projects related to the platforms.

First is getting the platforms themselves registered and regulated much like exchanges. Congress gave us a broad framework with which to regulate

exchanges. These crypto platforms play roles similar to those of traditional regulated exchanges. Thus, investors should be protected in the same way.

The U.S. has the greatest capital markets because investors have faith in them. We have rules with respect to safeguarding market integrity, protecting against fraud and manipulation, and facilitating capital formation. If a company builds a crypto market that protects investors and meets the gold standard of our market regulations, then customers will be more likely to trust and have greater confidence in that market.

In my view, regulation both protects investors and promotes investor confidence, in the same way that traffic laws protect drivers and promote driver confidence. It's at the core of what makes markets work.

Some have asked if the current exemptions for so-called alternative trading systems (ATSs) could be generally available to crypto platforms. ATSs for the equity and fixed income markets, though, are generally used by institutional investors.

This is quite different than crypto asset platforms, which have millions and sometimes tens of millions of retail customers directly buying and selling on the platform without going through a broker.

Thus, I've asked staff to consider whether and how the protections that are afforded to other investors on exchanges with which retail investors interact should apply to crypto platforms.

Second, crypto platforms currently list both crypto commodity tokens and crypto security tokens, including crypto tokens that are investment contracts and/or notes.

Currently, the venues that the SEC oversees solely trade securities. Thus, I've asked staff to consider how best to register and regulate platforms where the trading of securities and non-securities is intertwined.

In particular, I've asked staff to work with the Commodity Futures Trading Commission (CFTC) on how we jointly might address such platforms that might trade both crypto-based security tokens and some commodity tokens, using our respective authorities.

The third area is around crypto custody. Unlike traditional exchanges, currently centralized crypto trading platforms generally take custody of their customers' assets.

Last year, more than $14 billion of value was stolen. I've asked staff how to work with platforms to get them registered and regulated and best ensure the protection of customers' assets, in particular whether it would be appropriate to segregate out custody.

Further, unlike traditional securities exchanges, crypto trading platforms also may act as market makers and thus as principals trading on their own platforms for their own accounts on the other side of their customers. I've thus asked staff to consider whether it would be appropriate to segregate out market making functions.

As it relates to crypto lending platforms, we recently charged BlockFi with failing to register the offering of its retail crypto lending product, among other violations.

The settlement made clear that crypto markets must comply with time-tested securities laws, such as the Securities Act of 1933 and the Investment Company Act of 1940. It further demonstrates the Commission's willingness to work with crypto platforms to determine how they can come into compliance with those laws.

BlockFi agreed to attempt to bring its business into compliance with the Investment Company Act, and its parent company announced that it intends to register under the Securities Act of 1933 the offer and sale of a new lending product.

Stablecoins

The second area is the $183 billion (and growing) stablecoins market.[7] Outside of use on crypto platforms, stablecoins generally are not used for commerce. Generally, you're not using them to get a cup of coffee at Good Karma on your way to class from Center City. They are not issued by a central government and are not legal tender.

Stablecoins, though, in offering features similar to and potentially competing with bank deposits and money market funds, raise three important sets of policy issues.

First, stablecoins raise public policy considerations around financial stability and monetary policy.

Such policy considerations underlie regulations that banking regulators have with respect to deposits and that we at the SEC have with respect to money market funds and other types of securities. Many of those issues are discussed in the recent President's Working Group Report.

For instance, what backs these tokens so we can make sure that these holdings can actually be converted to dollars one-to-one? Further, stablecoins are so integral to the crypto ecosystem that a loss of the peg or a failure of the issuer could imperil one or more trading platforms, and may reverberate across the wider crypto ecosystem.

Second, stablecoins raise issues on how they potentially can be used for illicit activity. Stablecoins primarily are used for crypto-to-crypto transactions, thus potentially facilitating platforms and users avoiding or deferring an on-ramp or off-ramp with the fiat banking system.

Thus, the use of stablecoins on platforms may facilitate those seeking to sidestep a host of public policy goals connected to our traditional banking and financial system: anti-money laundering, tax compliance, sanctions, and the like.

Third, stablecoins raise issues for investor protection. Stablecoins were first adopted and continue to be dominantly used on crypto trading and lending platforms.

About 80 to 85 percent of trading and lending on these platforms involves stablecoins. When trading on a platform, the tokens actually often are owned by the platforms, and the customers just have a counterparty relationship with the platform.

The three largest stablecoins were created by trading or lending platforms themselves, and U.S. retail investors have no direct right of redemption for the two largest stablecoins by market capitalization.

There are conflicts of interest and market integrity questions that would benefit from more oversight.

Tokens

Then, thirdly from a policy perspective are all the other crypto tokens. The fact is, most crypto tokens involve a group of entrepreneurs raising money from the public in anticipation of profits — the hallmark of an investment contract or a security under our jurisdiction.

Some, probably only a few, are like digital gold; they may not be securities. Even fewer, if any, are actually operating like money.

When a new technology comes along, our existing laws don’t just go away.

In the 1930s, Congress painted with a broad brush the definition of a security. Our laws have been amended many times since then, Congress has painted with an even wider brush, and the Supreme Court has weighed in numerous time.

They've all said, basically, to protect the public against fraud, to protect the public against scammers, people raising money from the public had to register and make basic disclosures with a cop on the beat: the SEC.

You might wonder: how might a crypto token be a security?

The Supreme Court's 1946 Howey Test, which was about orange groves, says that an investment contract exists when there is the investment of money in a common enterprise with a reasonable expectation of profits to be derived from the efforts of others.

My predecessor Jay Clayton said it, and I will reiterate it: Without prejudging any one token, most crypto tokens are investment contracts under the Howey Test.

Even before the Howey test, in the first several years of our federal securities laws, some entrepreneurs were notified that they had to register their offerings of chinchillas, whiskey warehouse receipts, oyster beds, and live silver foxes as securities offerings, as "the purported sale of the…property was merely camouflage and not the substance of the transaction."

Today, many entrepreneurs are raising money from the public by selling crypto tokens, with the expectation that the managers will build an ecosystem where the token is useful and which will draw more users to the project.

Thus, it is important that we work to get crypto tokens that are securities to be registered with the SEC. Issuers of crypto tokens that are securities must register their offers and sales of these assets with the SEC and comply with our disclosure requirements, or meet an exemption.

Issuers of all kinds across a variety of markets successfully register and provide disclosures every day. If there are, in fact, forms or disclosure with which crypto assets truly cannot comply, our staff is here to discuss and evaluate those concerns.

Any token that is a security must play by the same market integrity rulebook as other securities under our laws.

Conclusion

In conclusion, new technologies come along all the time; the question is how we adjust to that new technology.

But make no mistake: We already live in a digital age. That's not what's new here. We already can buy a cup of coffee with money stored in an app on our smartphones.

The days of physical stock certificates ended decades ago. There's nothing new about people raising money to fund their projects. Crypto may offer new ways for entrepreneurs to raise capital and for investors to trade, but we still need investor and market protection.

We already have robust ways to protect investors trading on platforms. And we have robust ways to protect investors when entrepreneurs want to raise money from the public.

We ought to apply these same protections in the crypto markets. Let's not risk undermining 90 years of securities laws and create some regulatory arbitrage or loopholes.

Thank you.

You may visit:
https://www.sec.gov/news/speech/gensler-remarks-crypto-markets-040422

Number 3

Central bank digital currencies: a new tool in the financial inclusion toolkit?

FSI Insights No 41, by Raphael Auer, Holti Banka, Nana Yaa Boakye-Adjei, Ahmed Faragallah, Jon Frost, Harish Natarajan and Jermy Prenio

BIS

Executive summary

Central banks are actively considering how retail central bank digital currencies (CBDCs) may fit with policy goals around financial inclusion.

In the second half of 2021, authors at the BIS and the World Bank interviewed nine central banks at various stages of exploring retail CBDCs and financial inclusion.

These are the Central Bank of The Bahamas, Bank of Canada, People's Bank of China, Eastern Caribbean Central Bank, Bank of Ghana, Central Bank of Malaysia, Bangko Sentral ng Pilipinas, National Bank of Ukraine and Central Bank of Uruguay.

While a CBDC, like other forms of money, has different functions (eg means of payment, store of value, unit of account, settlement asset), its link to financial inclusion is in the context of its payment properties, and hence it is the lens through which CBDC is discussed in this paper.

The interviewed central banks take the view that, while CBDC is not a panacea, it can represent a further tool to promote financial inclusion if designed with this goal.

The paper explores this theme, outlining findings in three main areas:

(i) existing barriers to financial inclusion that could be addressed with the introduction of a CBDC;

(ii) CBDC design features that many jurisdictions view as critical to addressing these barriers; and

(iii) the challenges foreseen, along with legal and regulatory changes needed for CBDC implementation.

Barriers to financial inclusion differ across countries, but there were some common elements that came out in the interviews. These can be grouped into six main areas.

First are geographic barriers related to vast territories and remote locations.

Second are institutional and regulatory factors, such as a lack of public goods like identity credentials, as well as informality and a lack of consumer protection.

Third are economic and market structure issues, including limited competition, inefficiency in the financial sector and a lack of profitability of serving excluded groups.

Fourth are characteristics of vulnerability, such as barriers by age, gender, income or disability status like visual and hearing impairments.

Fifth is a lack of education and financial literacy, and sixth is low trust in existing financial services.

Some central banks consider CBDCs as key to their mandate as a catalyst for innovation and economic development.

While access to payment services has grown in recent years, it is still far from universal.

Low-income populations and those living in remote locations continue to confront barriers to digital payments.

Domestic retail payment services can be expensive, and payments across borders – particularly for low-value transfers like remittances – face even larger challenges.

CBDCs can secure the continuous provision of public money to the general public.

With CBDCs, central banks can help to speed up digital payment adoption, particularly when market size and profit potential are insufficient to motivate private sector innovation, or when established oligopolies prevent entry.

Some central banks argued that they have a role to play in applying innovation to specific access challenges.

As such, given the expanding yet uneven access to payment services, they recognise the importance of pursuing CBDC issuance.

Several central banks see CBDC more as a potential complement to existing financial inclusion initiatives.

Many jurisdictions are tackling financial inclusion barriers today with dedicated strategies to improve the provision of transaction accounts and other payment products. The entry of non-banks and agent-based models, risk-based and proportionate customer enrolment processes, effective use of data and interoperability remain relevant.

Authorities are already expanding the network of readily available access points and developing tools to improve awareness of transaction accounts and digital money, including by promoting financial and digital literacy.

Central banks are also modernising existing payment infrastructures with the introduction of fast payment systems and leveraging high-volume recurrent payment streams. Several central banks noted that these actions, if implemented effectively,
would be the most direct means to tackle financial exclusion.

These are in line with the Committee on Payments and Market Infrastructures and World Bank guiding principles of payment aspects of financial inclusion (PAFI).

To read more: https://www.bis.org/fsi/publ/insights41.pdf

Executive summary 1

Section 2 – Barriers to financial inclusion and policies to address them 4

Section 3 – Inclusive CBDC design 11

- Do CBDCs have a unique proposition with respect to financial inclusion? 11
- Insights from the central bank interviews 13
- Promoting innovation in a two-tiered payment system 15
- Offering a robust and low-cost public sector technological basis and novel interfaces 17
- Customer enrolment and education on the use of CBDC 20
- Fostering interoperability among multiple dimensions 23
- Summary: mapping specific design elements to financial inclusion barriers 26

Section 4 – Challenges, risks and legal/regulatory implications 27

- Challenges and risks 27
- Legal and regulatory implications 30

Section 5 – Conclusion 32

References 33

Number 4

COSTS AND PAST PERFORMANCE REPORT – 2022

Despite the unprecedented challenges posed by the COVID-19 pandemic, both the insurance and pension retail investment markets performed well.

Net returns were overall positive and in line with the five year trend.

The threat of rising inflation, however, represents an emerging risks to be monitored across the sector.

For the 2022 report EIOPA received information on:

- more than 760 *Insurance-based Investment Products (IBIPs),* marketed by 160 undertakings accounting for 60% of total Gross Written Premiums (GWP) in the European Economic Area;

- more than 200 *personal pension products (PPPs)* corresponding circa 0.8 million contracts;

- data on assets, expenses and income of European *Institutions for Occupational Retirement provision (IORPs).*

IBIPs offered steadily positive returns, with unit-linked products outperforming hybrid and profit participation products despite higher costs.

Data on ESG products, albeit not representative, shows strong performance.

IBIPs offered steadily positive valuation in 2020 with unit-linked products outperforming hybrid and profit participation products, while also carrying higher costs.

Unit-linked products return was 6.0% while hybrids and profit participation had a net return of 2.0% and 1.4% respectively.

A putative investor buying a unit-linked contract for € 10,000 in 2016 would have achieved a net value of € 12,564 at the end of 2022 (4.7% per year).

Hybrid and profit participation products' past performance, albeit more stable, was lower, being on average 2.5% for hybrid and 1.7% for profit participation products.

The shift from traditional profit participation products towards hybrid and unit-linked products observed in the past years accelerated in 2020, heightened by the market environment characterised by the pandemic and the prolonged low interest rate environment.

GWP corresponding to profit participation products decreased more than 10% in 2020.

Higher risk classes delivered higher levels of net returns for unit-linked and hybrid products while longer holding periods continue driving higher performance of profit participation products.

Products corresponding to lower risk classes had particularly low net returns, at times negative (ranging between -1% and 1%), questioning the value for money offered by these products.

Riskier unit-linked products provided higher returnsthan hybrid products, having paid an annualised return of ca. 10%, almost twice the annualised average net return corresponding to riskier hybrids.

For profit participation products longer holding periods remain a driver of extra performance, paying on average 1% more than products with shorter durations.

To read more:
https://www.eiopa.europa.eu/document-library/costs-and-past-performance-report/cost-and-past-performance-report-2022_en

Number 5

PCAOB Requests Comment on Impact of Auditing Requirements Related to Estimates and Specialists

Comments Due June 10, 2022

The Public Company Accounting Oversight Board (PCAOB) today issued a Request for Comment(PDF) on the initial impact of new requirements for auditing accounting estimates and using the work of specialists. You may visit:
https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/economicandriskanalysis/pir/documents/rfc-interim-analysis-estimates-specialists-audit-requirements.pdf?sfvrsn=b6e49df_2

The Request for Comment is a key part of the PCAOB's interim analysis of these requirements. The PCAOB will evaluate comments received, along with other evidence obtained from the analysis, and consider whether additional guidance or other steps may be appropriate.

"The PCAOB is committed to performing robust economic analyses of the overall effect of new auditing requirements, including performing post-implementation reviews," said PCAOB Chair Erica Y. Williams. "We welcome input from investors, audit committees, preparers, academics, audit firms, and others who use financial statements."

Comments can be submitted through the following methods:

- By email to comments@pcaobus.org;

- By postal mail to the Office of the Secretary, PCAOB, 1666 K Street, NW, Washington, DC 20006-2803.

All comments should refer to Interim Analysis No. 2022-001, Estimates and Specialists Audit Requirements, on the subject or reference line and should be submitted no later than June 10, 2022. Please note that comments will be posted to the PCAOB website.

Additional information on our interim analysis and specific questions for consideration are detailed in the Request for Comment(PDF) document. You may visit:
https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/economicandriskanalysis/pir/documents/rfc-interim-analysis-estimates-specialists-audit-requirements.pdf?sfvrsn=b6e49df_2

We encourage commenters to provide data, evidence, and/or specific examples in support of their comments. More information about the PCAOB's post-implementation review program is also available on the PCAOB website.

Questions for investors:

1. Do investors believe that the new requirements for auditing accounting estimates, including fair value measurements, contribute to an increase in audit quality? Why or why not?

2. Have the new requirements improved investor confidence in financial statements? Have the new requirements reduced investor uncertainty about audit quality and potential risks associated with accounting estimates?

3. What other benefits, if any, have investors experienced as a result of the new requirements? Do investors believe that the overall benefits of the new requirements outweigh their costs?

Questions for auditors, audit committee members, and financial statement preparers:

1. How did audit firms approach implementation of the new requirements for auditing accounting estimates, including fair value measurements? What were the most significant activities that firms undertook to support and monitor implementation of the new requirements by individual audit engagement teams?

2. To what extent did the new requirements lead to changes in auditing practice? How did the impact of the new requirements vary across audit firms and audit engagements? Please describe any changes to auditing practice and provide perspectives on the associated implications for audit and financial reporting quality.

3. To what extent did the new requirements have implications for communication and dialog between auditors, audit committees, and preparers? Please describe any changes and associated implications for audit and financial reporting quality.

4. What costs did audit firms incur to implement the new requirements? Did the new requirements generate any efficiencies? Please describe and estimate costs/efficiencies directly related to implementation of the new requirements, distinguishing between one-time and recurring costs/ efficiencies. For recurring costs/efficiencies, please state whether you believe the costs/efficiencies will increase, decrease, or not change in future years.

5. Did audit fees change because of the new requirements? To what extent were any additional fees due to the new requirements versus other contemporaneous environmental factors (e.g., new accounting requirements or the COVID-19 pandemic) that may have influenced audit effort? What other costs, if any, did companies experience directly related to the new requirements?

6. Did audit firms encounter any significant challenges in implementing the new requirements? If so, please describe and, if applicable, please reference the specific requirements that caused the challenges.

7. Did the new requirements give rise to any unintended consequences? Please describe any unintended consequences and, if applicable, reference the specific requirements that caused them.

To read more:
https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/economicandriskanalysis/pir/documents/rfc-interim-analysis-estimates-specialists-audit-requirements.pdf?sfvrsn=b6e49df_2

Number 6

Cybersecurity Market Analysis in support of Informed Cybersecurity Business Decisions

The European Union Agency for Cybersecurity (ENISA) introduces a framework to perform cybersecurity market analyses and dives into the market of the Internet of Things (IoT) distribution grids for validation.

What's the objective?

To improve market penetration, value for money, quality and acceptance of products, processes and services, performing cybersecurity market analysis has become an important tool for a variety of stakeholders.

Market data is currently considered key to making informed decisions related to cybersecurity choices, on new products to be launched, policy initiatives or research and innovation funding.

The first report introduces a market analysis framework to be applied across various application areas over time.

The second report analyses the IoT cybersecurity market demand and supply in the sector of electricity distribution grids across the EU.

How does the framework work?

The framework consists of a toolbox designed to facilitate the performance of cybersecurity market analyses. It offers a range of analysis approaches based on innovative market modelling specifically adapted to the cybersecurity market.

This framework can be applied to various market segments. Structured around six modules, it offers the flexibility to choose the type of the performed analysis among:

- Market structure & segmentation;
- Demand-side research;
- Supply-side research including vendor market map;
- Technology research;
- Macro-environmental factors and
- Economic market characteristics.

Main points and foreseen next steps:

- On the framework

Identifying the right data and the right method to perform data collection is essential if we want to avoid pitfalls such as bias.

The processing techniques currently available need to be assessed and selected wisely.

Moreover, the confidentiality of market data collected also raises both competition, and technical questions to be addressed.

They call for the use of anonymisation, implementing security controls, etc.

The framework introduces a coherent taxonomy of cybersecurity products, processes and services.

This cybersecurity taxonomy has been derived from relevant work already performed within the EU.

Cooperation with stakeholders that are active in classifying cybersecurity has also been taken into account (e.g. European Commission's Joint Research Centre).

Furthermore, Member States already started implementing cybersecurity market surveillance functions.

These functions aim to check whether ICT products comply with the requirements of EU cybersecurity certificates.

The development of market surveillance in Member States has been identified as a priority for ENISA today and for the years to come.

The proposed cybersecurity market analysis framework may be a useful input to these efforts.

- On IoT in distribution grids

The analysis on IoT for electricity grids reveals that the architecture of distribution grids is undergoing some major changes.

Flexible and dynamically configured bi-directional power flows are gradually replacing traditional, one-way transmission electricity grids.

The digital transformation of electricity grids will imply investing in digitalised components. However, this digitalisation will in turn lead to more cyber threat exposure by adversaries, such as State or non-State actors.

The report on IoT serves as a proof of concept of the initial cybersecurity market analysis framework published herewith. Part of the objective of this report was to validate the applicability of the proposed framework.

With the support of the Ad Hoc Working Group (AHWG) on the EU Cybersecurity Market established by ENISA in 2021, the Agency will conduct additional cybersecurity market analyses to further develop the framework.

To read more:
https://www.enisa.europa.eu/news/enisa-news/cybersecurity-market-analysis-in-support-of-informed-cybersecurity-business-decisions

Number 7

ENISA Cybersecurity Market Analysis Framework (ECSMAF)

This document is the cornerstone of ENISA activities in analysing the EU cybersecurity market: it presents a cybersecurity market analysis framework as a "cookbook" on how EU cybersecurity market analyses can be performed.

1. INTRODUCTION 6

1.1 POLICY CONTEXT 6

1.2 PURPOSE, OBJECTIVES AND SCOPE 8

1.3 TARGET AUDIENCE 9

1.4 STRUCTURE OF THE REPORT 11

2. CONTENT OF THE ENISA CYBERSECURITY MARKET ANALYSIS FRAMEWORK (ECSMAF) 12

2.1 LOGICAL BLOCKS/MODULES OF ECSMAF 12

2.1.1 Market structure and segmentation 13
2.1.2 Demand-side research 15
2.1.3 Supply-side research 17
2.1.4 Technology research 19
2.1.5 Macro-Environmental Factors and Economic Market Characteristics 21

2.2 CONTEXTUALIZED ECSMAF COMPONENTS 23

2.2.1 Scoping the analysis and ECSMAF parametrization 24
2.2.2 Cybersecurity market taxonomy 26
2.2.3 Cybersecurity market trends 31
2.2.4 Market stakeholder types 32
2.2.5 Methods for collecting market data 34

3. RELATED AREAS 36

4. ISSUES, CONSIDERATIONS, CONCLUSIONS 40

4.1 GENERAL REMARKS 40

4.2 OPEN ISSUES AND WAYS FORWARD 41

A ANNEX: EXAMPLES 43

A.1 EXAMPLES OF MARKET STRUCTURE AND SEGMENTATION 43

A.2 EXAMPLES OF DEMAND-SIDE RESEARCH 44

A.3 EXAMPLES OF SUPPLY-SIDE RESEARCH 45

A.3.1 Example of Market Map 45

A.4 EXAMPLES OF TECHNOLOGY RESEARCH 46

A.4.1 Example of Scenarios and Technology Map 46
A.4.2 Example of market adoption forecast 47

A.5 EXAMPLES OF MACRO-ENVIRONMENTAL FACTORS AND ECONOMIC MARKET CHARACTERISTICS 48

B MAIN ABBREVIATIONS 50

In 2021, in its efforts to contribute to the achievement of its objectives as defined in the Cybersecurity Act (CSA) and to the implementation of the ENISA Single Programming Document, ENISA has kicked-off a series of activities in the area of cybersecurity market analysis.

Analysing how well cybersecurity products, services and processes succeed in the market is a key step in understanding how to improve their market diffusion, importance, quality and acceptance.

Though cybersecurity has been considered in the past within market analysis efforts, the customisation and scoping of cybersecurity market analyses is still at low levels of maturity.

Moreover, market data on cybersecurity products, services and processes are scarcely taken into account in the cybersecurity development life-cycle, e.g. within decision-making processes for the launching and development of cybersecurity initiatives, product ideas, policy actions, research funding, and deployments.

By initiating this activity, ENISA delivers an important contribution towards a more targeted, market-driven decision-making process for the conception, launching and maintenance of cybersecurity products, services and processes within the EU.

This document is the cornerstone of ENISA activities in analysing the EU cybersecurity market: it presents a cybersecurity market analysis framework as a “cookbook” on how EU cybersecurity market analyses can be performed and be:

- More transparent: the fact that analysis method, parametrization, cybersecurity value chain, market trends and market stakeholders are fixed, leads to a more transparency as regards the results of the analysis.

- More comparable: by having set both the content of various components and the steps of the analysis process, the achieved results are more comparable, and thus reusable among various analyses performed.

- More targeted towards specific cybersecurity value chains: the availability of a standard taxonomy of cybersecurity value chains, allows for more targeted analysis with regard to specific cybersecurity areas, products, services and processes.

- More customizable towards technology and market trends: the possibility to customize an analysis according to various trends, allows

for consideration of market dynamics by means for forecasts, market gaps and market niches.

- More agile: the inherent flexibility of setting market analysis foci and adapting accordingly the performed analysis process, increases agility of the proposed market analysis method.

- More comprehensive: the inclusion of all possible variables, criteria and contextual information on cybersecurity, as well as requirements and dependencies both from the supply and the demand sides, increases the comprehensiveness of the proposed market analysis method.

- More coherence: the use of the framework to perform market analyses facilitates information exchanges among specific market analysis reports by means of re-usability and coherence of created/maintained market information (both raw market data and analysis results).

The framework presented in this report is at its initial development phase. With increasing performance of cybersecurity market analyses, but also with interactions with stakeholders, ENISA will continuously develop, update and maintain the current framework to increase its efficiency and practicability. To this extent, it constitutes rather the starting point of a journey than a destination.

You may visit:
https://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysis-framework-ecsmaf

Figure 1: Logical blocks/modules of ECSMAF

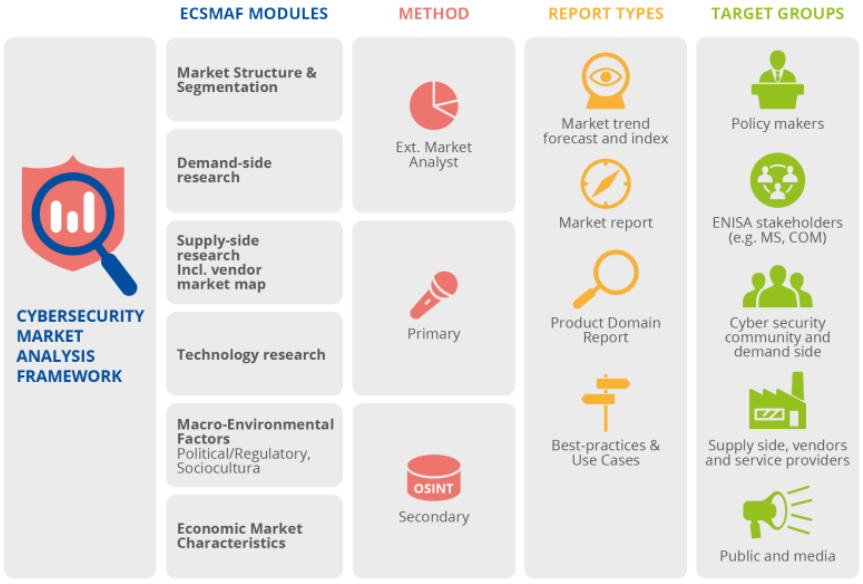
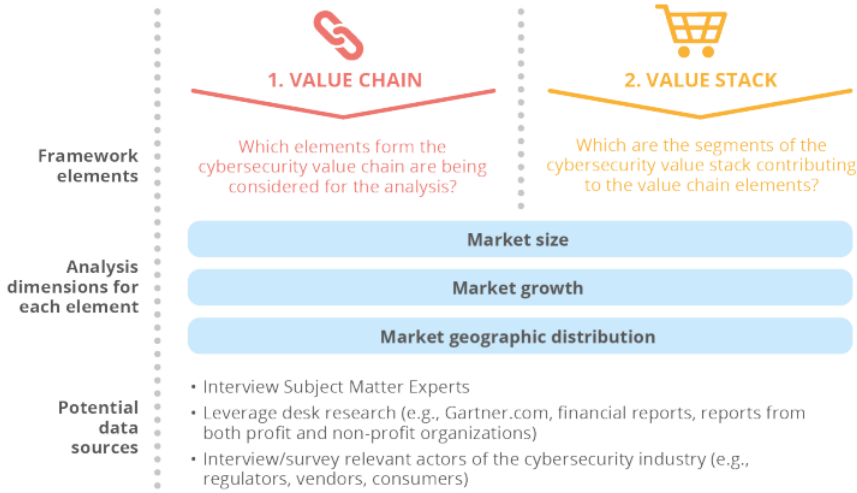


Figure 2: Structure and steps within the module Market Structure and Segmentation



Number 8

Environmental, Social and Governance (ESG) risks

EBA publishes binding standards on Pillar 3 disclosures on ESG risks

▪ The technical standards aim to ensure that stakeholders are well-informed about institutions' ESG exposures, risks, and strategies and can make informed decisions and exercise market discipline.

▪ The standards put forward comparable disclosures and KPIs, including a green asset ratio (GAR) and a banking book taxonomy alignment ratio (BTAR), as a tool to show how institutions are embedding sustainability considerations in their risk management, business models and strategy and their pathway towards the Paris agreement goals.

▪ In developing this framework, the EBA has built on the recommendations of existing initiatives, like those of the Task Force on Climate-related Financial Disclosures (TCFD) of the Financial Stability Board (FSB), but has gone beyond by defining binding granular templates, tables and instructions, to ensure enhanced consistency, comparability and meaningfulness of institutions' disclosures.

The European Banking Authority (EBA) published its *final draft* implementing technical standards (ITS) on Pillar 3 disclosures on Environmental, Social and Governance (ESG) risks.

The final draft ITS put forward comparable disclosures to show how climate change may exacerbate other risks within institutions' balance sheets, how institutions are mitigating those risks, and their ratios, including the GAR, on exposures financing taxonomy-aligned activities, such as those consistent with the Paris agreement goals.

Disclosure of information on ESG risks is a vital tool to promote market discipline, allowing stakeholders to assess banks' ESG related risks and sustainable finance strategy.

The EBA ESG Pillar 3 package will help to address shortcomings of institutions' current ESG disclosures at EU level by setting mandatory and consistent disclosure requirements, including granular templates, tables and associated instructions.

It will also help establish best practices at an international level.

In line with the requirements laid down in the Capital Requirements Regulation (CRR), the draft ITS set out comparable quantitative disclosures on climate-change related transition and physical risks, including information on exposures towards carbon related assets and assets subject to chronic and acute climate change events.

They also include quantitative disclosures on institutions' mitigating actions supporting their counterparties in the transition to a carbon neutral economy and in the adaptation to climate change.

In addition, they include KPIs on institutions' assets financing activities that are environmentally sustainable according to the EU taxonomy (GAR and BTAR), such as those consistent with the European Green Deal and the Paris agreement goals.

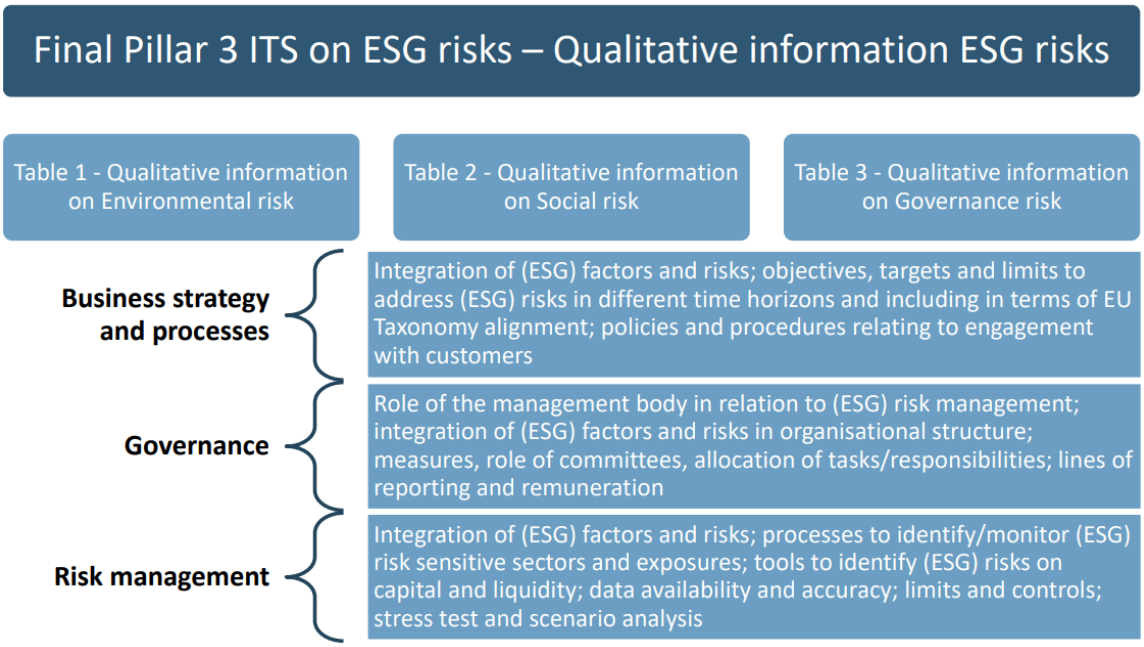
Finally, the final draft ITS provide qualitative information on how institutions are embedding ESG considerations in their governance, business model, strategy and risk management framework.

The EBA has integrated proportionality measures that should facilitate institutions' disclosures, including transitional periods and the use of estimates.

The Pillar 3 disclosure framework promotes transparency as a main driver of market discipline in the financial sector, to reduce the asymmetry of information between credit institutions and users of information, and to address uncertainties on potential risks and vulnerabilities faced by institutions.

The Pillar 3 framework on prudential disclosures on ESG risks is intended to allow investors and stakeholders to compare the sustainability performance of institutions and of their financial activities, and will support institutions in the public disclosure of meaningful and comparable information on how ESG-related risks and vulnerabilities, including transition and physical risks, may exacerbate other risks in their balance sheet.

In addition, it will help institutions in providing transparency on how they are mitigating those risks, including information on how they are supporting their customers and counterparties in the adaptation process to e.g. climate change and in the transition towards a more sustainable economy.



To read more:
https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Draft%20Technical%20Standards/2022/1026171/EBA%20draft%20ITS%20on%20Pillar%203%20disclosures%20on%20ESG%20risks.pdf

Number 9

Balancing on the net-zero tightrope

Sarah Breeden, Executive Director for Financial Stability Strategy and Risk and a member of the Financial Policy Committee (FPC) in UK.

Let's be frank. This is not the start to the 2020s that we had all hoped for. A global pandemic followed by tragedy in Ukraine has led to unimaginable human suffering. And the collective toll on our livelihoods and economies has been at a scale rarely seen.

Of the many lessons we have learned from these crises, one has particular relevance when considering the risks to the financial system from climate change and the transition to net-zero emissions: that managing sharp adjustments in the economy is never easy.

Sudden and large rises in the prices of key commodities, such as oil, natural gas and wheat, are contributing to economic and financial disruption for households, businesses and governments around the world.

It reminds us that if we want to minimise risks and maximise opportunities, we need to act early to assess the risks and build resilience against future shocks, whether from pandemics, geopolitical events, or the transition to net-zero.

The harder question is how we all – governments, central banks, financial institutions and business – manage the trade-offs we will face along the way. Those trade-offs are environmental and economic, as well as political, social, and distributional.

Managing these effectively is like walking on a tightrope – with a need to maintain the right balance. Or put another way, it's not just the destination (net zero by 2050) that matters, the journey (our transition pathway) is important too.

In the end, the path we take for our planet, economy, and financial system, will ultimately be the sum of myriad individual decisions, not just big commitments.

We must make those decisions in a timely and informed way with a good understanding of both the intended and unintended consequences they

could create. That is what I would like to explore today. How can we balance on the net-zero tightrope and what role can the Bank of England, working closely with government, play in keeping us steady.

The Bank of England's role

Let me start with the Bank of England's role.

As the UK's central bank and prudential regulator, the Bank's role in the transition is to understand how different transition pathways could affect the macroeconomy, the stability of the wider financial system, and the safety and soundness of the firms we regulate.

Our policy response must be calibrated to address the risks that these pathways pose to our objectives. The Bank's actions can also help magnify the effects of government climate policyfootnote, not least since a resilient financial system will be better able to support the transition.

Mitigating climate change and solving for the transition is ultimately going to take the combined efforts of government, industry, finance, regulators, and individuals. But while we may all have a role to play, it is important to remember that they are not the same roles, and that action by one cannot necessarily substitute for inaction by another. Financial regulations cannot substitute for government climate policies, and consumer spending choices cannot substitute for public and private investment.

Climate action by financial firms

That brings me to the financial sector.

A lot has changed in the past few years. We are seeing firms begin to make more serious investments in developing effective capabilities both to manage climate-related financial risks and to identify the opportunities from the transition, whether through more sophisticated climate data analytics or setting firm specific net-zero strategies.

Regulators like us have played a part in prompting this shift, but so too have the demands and needs of investors and customers. We have seen progress, which is welcome. However there is still much further to go before capabilities can be considered effective and firms' actions sufficient to support the transition.

The financial sector's role in the transition is clear. It must facilitate the flow of finance to support businesses and households in reducing their emissions and help smooth the adjustment in the real economy.

But there is a problem.

External scrutiny on firms' climate actions is increasing, but this tends to focus on their individual actions and the greenness of their lending and investments today, rather than the aggregate outcomes which determine the climate future we face. This approach may lead to firms greening their own balance sheets today, not greening the future wider economy. And yet the latter is what is ultimately needed to reach net-zero emissions.

The 'own balance sheet' approach may lead firms or their stakeholders to conclude that they should simply divest from emissions-intensive companies, assets and jurisdictions.

While this balance sheet-greening – or paper decarbonisation – may reduce the direct risks firms face from transition, it will not reduce the system-wide risks we will all face, unless those actions mean that emissions are actually reduced. Put another way, anything one firm does to green its own balance sheet will be undermined where those emissions-intensive activities can continue to be financed by alternative sources that will not steward them toward net-zero.

Finance needs to support an economy comprised of both green and greening firms. Importantly, it also needs to address not only energy supply, but energy demand through improved energy efficiency. Indeed this week's *IPCC report* in a new window revealed that modelled finance flows for climate mitigation over this decade need to be as much as six times higher than current levels if we are to limit warming to 1.5°C.
You may visit:
https://www.ipcc.ch/report/sixth-assessment-report-working-group-3/

Many firms have recognised this and are increasingly adopting active engagement and stewardship strategies to finance the changes that are needed. Where this is managed well and there is accountability for delivering change, the results can yield real world impact above and beyond those that divestment alone can deliver.

The shape and speed of the transition – the signposts for us to follow if you like – is for government to determine. But it is subject to uncertainty, and the need to recalibrate, given the long horizons involved. Indeed recent events – and the consequent volatility in energy prices – suggest that our path to net zero will be bumpier than we would otherwise have expected.

But uncertainty over climate policy cannot be an excuse for inaction by the real economy or financial sector. The calls for immediate actionOpens in a

new window from experts to reduce our future risks get ever louder. So we must recognise the need to use climate scenario analysis to explore a range of possible futures as we determine our actions today.

Our Climate Biennial Exploratory Scenario exercise – the results of which we will publish next month – is designed to do exactly that. We must use exercises like these to help us fulfil our collective responsibility to manage those bumps well.

The particular size, mix and timing of policy actions, and how they vary across jurisdictions, will of course have different impacts on different economic sectors and households.

Transition to net zero will create new winners and new losers; some will be better off and others will be worse.

Addressing these distributional effects through a just transition is not the responsibility of central banks and prudential regulators. But through our analysis we can help shine a light on those impacts and so support others (government, industry and investors) in their actions.

Unintended consequences

In addition to the intended consequences of policy choices and actions, we may also face unintended consequences. I want to draw your attention to three that I think we need to be mindful of.

First, there are policy choices, which could lead to a less effective transition.

I have already mentioned the potential for emissions-intensive activities to migrate outside of the banking sector.

That may lead to less transparency over these activities and could potentially deprive those firms that need to transition the most access to affordable finance.

That does not mean we should not take necessary actions in the banking sector.

But it does highlight that financial rules are limited by regulatory perimeters.

Second, rapid changes in the prices of green and emissions-intensive assets could lead to market instability.

The rush for green investment could create green asset bubbles and increase the risk of sudden price corrections, especially if greater demand for such investments incentivises greenwashing.

On the other side, sudden imposition of climate policies in a late and disorderly transition scenario could lead to a climate 'Minsky moment', where prices of emissions-intensive assets collapse, perhaps with wider financial and economic consequences.

Third, care must be taken in managing the transition to avoid unwarranted economic, social and distributional consequences.

We could see this occur where finance becomes the limiting factor for the provision of certain products or services, restricting their supply before a sustainable replacement has become available.

That might arise if limits on finance to corporates involved in the supply of high carbon energy runs ahead of replacement renewable sources. Or if there are restrictions on the provision of mortgages on energy inefficient buildings without finance available to improve them.

Credit being withdrawn can have wider consequences – for energy prices and the macroeconomy more broadly.

And as recent experience of higher energy prices has reminded us, these impacts can fall disproportionately on some groups.

Where do we go from here?

We stand at a crucial moment in the transition where momentum is with us but the transition risks being shaped by firms who are acting with limited information and with the potential for complex unintended consequences.

Successfully navigating this means we could be on a path to an orderly transition. Failing to transition in the right way may lead risks to crystallise, the consequences of which could fall hardest on the most vulnerable.

So how do we ensure that we stay steady as we balance the net-zero tightrope?

An effective transition requires the efficient allocation of capital to assets that are both green now and those that need greening, and the responsible retirement – over time – of assets which are not compatible with a net-zero outcome.

Greater detail on government climate policies will support this. But in the meantime greater transparency on firms' approaches to climate change through disclosures and transition plans is key to enabling the right action.

We have the foundations for that transparency through the Taskforce for Climate-Related Financial Disclosures (TCFD) and now the IFRS's International Sustainability Standards Board (ISSB).

On that note, I want to take the opportunity to welcome the UK Government's Sustainable Finance Roadmap and the Chancellor's commitment to a net zero aligned financial system, which includes moving to make disclosure of transition plans mandatory.

In addition, in the UK the Climate Financial Risk Forum (CFRF), the industry group which we co-chair with the FCA, will be making the transition a key area of its work going forwards.

Transition plans, as part of high quality and comparable climate disclosures, will assist investors and stakeholders to understand how firms are tackling the challenges of climate change.

Crucially they will set out what action is being taken to transition or adapt emission intensive assets and activities. That will aid the timely allocation of capital to invest not only in assets that are green now, but also to facilitate the provision of transition finance in support of activities that seek to reduce their impact on the climate over a responsible timeframe.

And as you may expect from the Bank, we have work underway to monitor and assess the transition to net zero and to understand how the characteristics could pose risks to monetary and financial stability, including those I have mentioned today.

Conclusion

I want to conclude by emphasising the point I made at the start. The transition to net zero is not a destination, it's a journey, and the path we take matters. Given recent events, that path might not be as direct as we might have hoped.

The urgent need for climate action is hard to overstate. But that should not mean we ignore the financial, economic, and social consequences that come with our choices as we balance on the net-zero tightrope.

Let me end with a positive.

Financial regulators' approach to climate change has been developed at pace. A process that ordinarily would have taken a decade or more to develop has happened in under half that time. The same is true of the international work on disclosures.

Both remind us of just how much progress has been made recently. That's a sentiment not often associated with climate change, but one we must build on. After all, there is no safety net if we fall.

The views expressed here are not necessarily those of the Financial Policy Committee. I am grateful to Andrew Bailey, Zane Jamal, Timothy Rawlings, Theresa Löber, Chris Faint, and Tom Daniels for their assistance in drafting these remarks.

Number 10

Hounding scammers with litigation

lbert Shin, Manager, CyberCrime Investigation Group
Mike Trinh, Senior Counsel

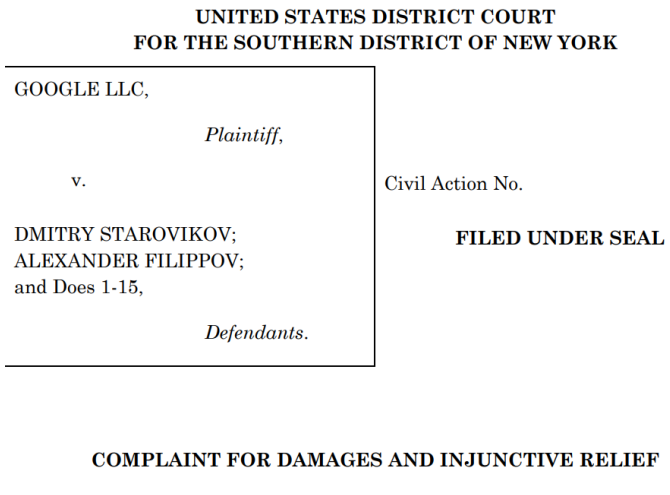
Google

Over the last few years we've seen a rise in bad actors using the internet for illegal activities, and we see it in our work.

Every single day we stop more than 100 million harmful emails from reaching our users, and we routinely work with law enforcement to combat nefarious actors.

But across the web, people are caught in romance scams, loan scams, and investment scams every day — and older Americans are often the most vulnerable.

Raising public awareness can help people avoid becoming victims. But for more emergent illicit behaviors and scams, lawsuits are an effective tool for establishing a legal precedent, disrupting the tools used by scammers, and raising the consequences for bad actors.



UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC,

Plaintiff,

v.

DMITRY STAROVIKOV;
ALEXANDER FILIPPOV;
and Does 1-15,

Defendants.

Civil Action No.

FILED UNDER SEAL

COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF

That's why last December we used our resources to file a lawsuit to combat illegal activity in the botnet industry and have used legal action to defend small businesses from scammers masquerading as Google.

With these actions, we establish legal precedent to help stop similar cyber threats and scams.

Today, we're building on this work by taking legal action against an actor who was operating fraudulent websites and using Google products as a part of their scheme.

The actor used a network of fraudulent websites that claimed to sell basset hound puppies — with alluring photos and fake customer testimonials — in order to take advantage of people during the pandemic.

This type of scheme follows a similar script to many online scams where malicious actors pretend to be someone they are not to convince victims to give them money for something they will never receive.

The Better Business Bureau recently announced that pet scams now make up 35% of all online shopping scams reported to them, and this particular scam targeted people at their most vulnerable, just as the pandemic led to a record spike in people wanting to own pets. (According to Google Search Trends, searches for "Adopt a Dog" spiked at the start of the pandemic as people spent more time at home. By the end of 2020, 70% of Americans reported owning a pet.)

Sadly, this scam disproportionately targeted older Americans, who can be more vulnerable to cyberattacks. The FTC and FBI report that older people are scammed out of an estimated $650 million per year.

That's why we're taking proactive action to set a legal precedent, protect victims, disrupt the scammer's infrastructure, and raise public awareness. Of course, legal action is just one way we work to combat these types of scams.

We build our security into all of our products and use machine learning to filter new threats, and our CyberCrime Investigation Group investigates misconduct and sends referrals to various law enforcement agencies including the Department of Justice to combat nefarious actors engaging in a wide range of scams including pets, covid relief, romance, and tech support scams.

Here are some additional steps you can take to help spot a pet scam:

- See the pet in person (or on a video call) before paying any money. This way, you are able to see the seller and the actual pet for sale. More often than not, scammers won't comply with the request.

- Use verified payment methods. Avoid wiring money or paying with gift cards or prepaid debit cards. And before you pay, research prices for

what you're looking to purchase. If someone is advertising a product at a deeply discounted price, you could be dealing with a fraudulent offer.

- Reverse image search. Search to see if the item or product is a stock image or stolen photo. Using Google Chrome, place the cursor over the photo and right click, then choose the option "Search Google for image." If that picture shows up in a number of places, you're likely dealing with a scam.

- Search online for the seller. Ask for the company name, number and street address. See what Google search results pop up. If you can't find anything, the name and address are likely fake.

We will continue to work with federal and state agencies and law enforcement to ensure our consumers are better protected from fraud online.

You may visit:
https://www.blog.google/technology/safety-security/hounding-scammers-litigation/
https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/1_Complaint.pdf

Plaintiff Google LLC ("Google") for its Complaint against the Defendants listed below alleges as follows:

INTRODUCTION

1. Defendants are Russian cybercriminals who have silently infiltrated more than a million computers and other devices around the globe to create a network—the Glupteba "botnet"—to use for illicit purposes, including the theft and unauthorized use of Google users' login and account information. Defendants use the Glupteba botnet to further a range of cybercrimes and to conceal criminal conduct. And at any moment, the power of the Glupteba botnet could be leveraged for use in a powerful ransomware[1] or distributed denial-of-service ("DDoS") attack.[2]

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 individual or entity;

- should not be relied on in the 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 regarding such problems incurred because of using this site or any linked external sites.

International Association of Risk and Compliance Professionals (IARCP)

You can explore what we offer to our members:

1. *Membership* – Become a standard, premium or lifetime member.

You may visit:
https://www.risk-compliance-association.com/How_to_become_member.htm

2. *Weekly Updates* - Visit the *Reading Room* of the association at:
https://www.risk-compliance-association.com/Reading_Room.htm

3. *Training and Certification* – Become:

- a Certified Risk and Compliance Management Professional (CRCMP),

- a Certified Information Systems Risk and Compliance Professional (CISRCP),

- a Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P,

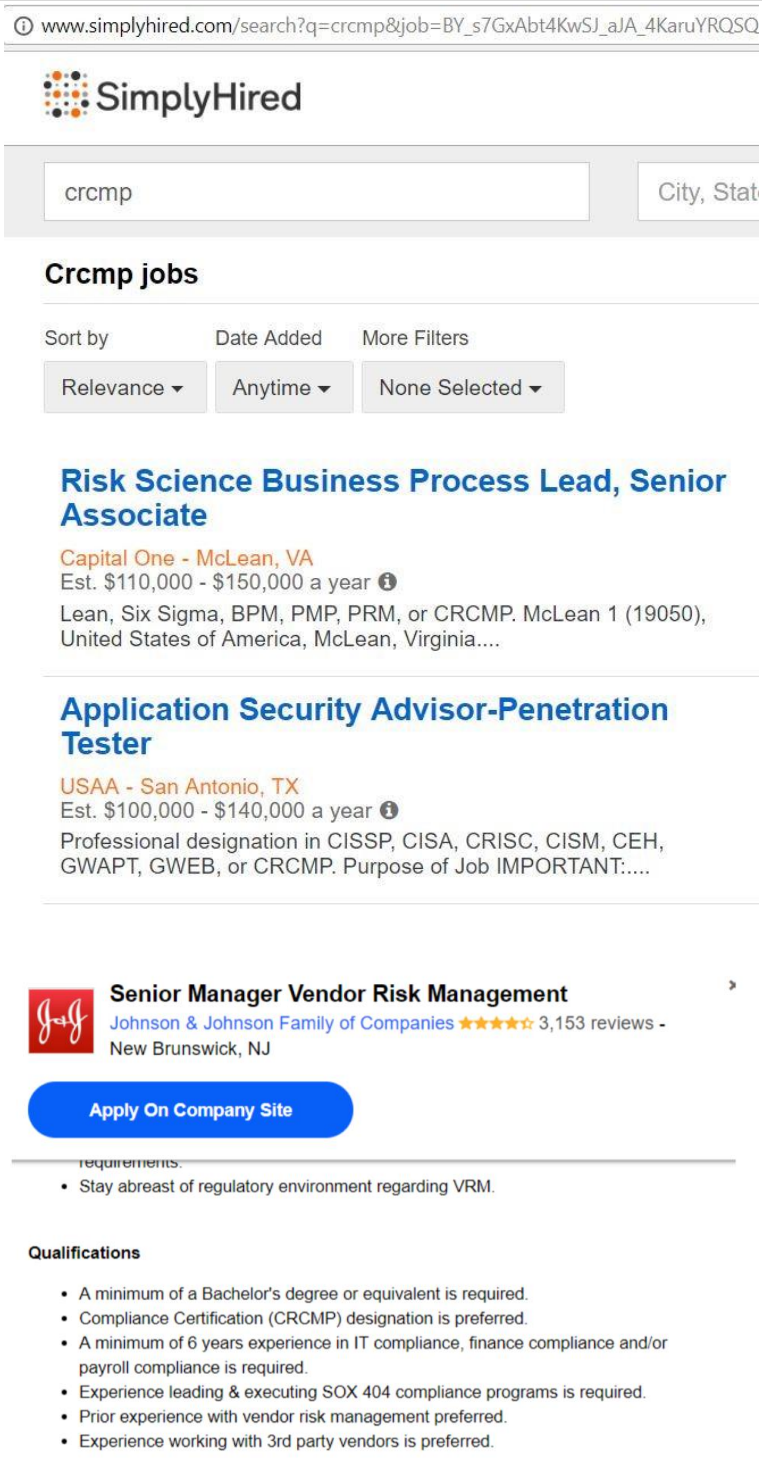
- a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I,

- a Travel Security Trained Professional (TSecTPro).

The CRCMP has become one of the most recognized certificates in risk management and compliance. There are CRCMPs in 32 countries.

Companies and organizations around the world consider the CRCMP a preferred certificate:

Senior Information Security Risk Analyst
Public Company Accounting Oversight Board - ★★★★☆ 10 reviews - Washington, DC
Professional designation in CISSP, CISA, CRISC, or CRCMP preferred. The PCAOB is a nonprofit corporation established by Congress to oversee the audits of public...



You can find more about the demand for CRCMPs at:
https://www.risk-compliance-association.com/CRCMP_Jobs_Careers.pdf

For the Certified Risk and Compliance Management Professional (CRCMP) distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/Distance_Learning_and_Certification.htm

For the Certified Information Systems Risk and Compliance Professional (CISRCP), distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CISRCP_Distance_Learning_and_Certification.htm

For the Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P, distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CC_GRC_P_Distance_Learning_and_Certification.htm

For the Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CRCMP_Re_I.htm

For the Travel Security Trained Professional (TSecTPro), distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/TSecTPro_Distance_Learning_and_Certification.htm

Certified Cyber (Governance Risk and Compliance) Professionals - CC(GRC)Ps, have a 50% discount for the Travel Security Trained Professional (TSecTPro) program ($148 instead of $297).

You have a $100 discount after you purchase one of our programs. The discount applies to each additional program. For example, you can purchase the CRCMP program for $297, and then purchase the CISRCP program for $197 (instead of $297), the CC(GRC)P program for $197 (instead of $297), the CRCMP(Re)I program for $197 (instead of $297), and the TSecTPro program for $197 (instead of $297).

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