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, October 25, 2021

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,

On October 2020, we had an interesting Final Report and High-Level Recommendations from the Financial Stability Board (FSB) with title *"Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements"*.

We read that the so-called "stablecoins" are a specific category of crypto-assets which have the potential to enhance the efficiency of the provision of financial services, but may also generate risks to financial stability, particularly if they are adopted at a significant scale.

According to the recommendations, while such financial stability risks are currently limited by the relatively small scale of these arrangements, this could change in the future. Stablecoins are an attempt to address the high volatility of "traditional" crypto-assets by tying the stablecoin's value to one or more other assets, such as sovereign currencies.

They have the potential to bring efficiencies to payments (including cross-border payments), and to promote financial inclusion. However, a widely adopted stablecoin with a potential reach and use across multiple jurisdictions (so-called "global stablecoins" or GSCs) could become systemically important in and across one or many jurisdictions, including as a means of making payments.

Today we have the *Progress Report on the implementation of the FSB High-Level Recommendations*. The report notes that, overall, the implementation of the FSB high-level recommendations across jurisdictions is still at an early stage. Jurisdictions have taken, or are considering, different approaches towards implementing the high-level recommendations, which could give rise to the risk of *regulatory arbitrage* and harmful market fragmentation.

The report also notes that standard-setting bodies, including BCBS, CPMI, and IOSCO are assessing whether and how existing international standards and principles may apply to stablecoin arrangements and adjusting them in light of the FSB high-level recommendations. The report stresses that a number of issues may not be fully covered by existing standards and principles and that gaps should be addressed in a holistic manner that is coordinated across sectors.

Authorities have identified several issues relating to the implementation of the recommendations that may warrant further consideration and where further work at international level could be useful.

These include:

- conditions for qualifying a stablecoin as a "global stablecoin";
- prudential, investor protection, and other requirements for issuers, custodians, and providers of other global stablecoin functions (e.g. wallet providers);
- redemption rights;
- cross-border and cross-sectoral cooperation and coordination; and
- mutual recognition and deference.

The FSB will undertake a review of its recommendations in consultation with other relevant SSBs and international organisations. The review, which will be completed in July 2023, will identify how any gaps could be addressed by existing frameworks and will lead to the update of the FSB's recommendations if needed.

According to the report, at present, stablecoins are being used primarily as bridge between traditional fiat currencies and other crypto-assets, which in

turn are primarily held and traded for speculative purposes. Increased participation by retail investors could give rise to broader financial stability issues through an erosion of trust in the financial system.

In the event that a stablecoin does enter the mainstream of the financial system as a means of payment and/or a store of value in multiple jurisdictions, with the potential to achieve substantial volume, it could become a *global stablecoin (GSC)*.

The emergence of GSCs would pose greater risks to financial stability than existing stablecoins and may challenge the comprehensiveness and effectiveness of existing regulatory, supervisory and oversight approaches.

Ensuring appropriate regulation, supervision and oversight across sectors and jurisdictions will therefore be necessary to prevent any potential gaps and avoid *regulatory arbitrage*.

Read more at number 3 below. Welcome to our 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 6)

Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative

Number 2 (Page 8)

Building Climate Scenario Analysis on the Foundations of Economic Research

Governor Lael Brainard, at the 2021 Federal Reserve Stress Testing Research Conference, Federal Reserve Bank of Boston, Boston

Number 3 (Page 12)

Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements

Progress Report on the implementation of the FSB High-Level Recommendations

Number 4 (Page 16)

PLI Broker/Dealer Regulation and Enforcement 2021

Gurbir Grewal, Director, Division of Enforcement, Washington D.C.

Number 5 (Page 24)

Agency Actions Needed to Address Foreign Influence

US Government Accountability Office (GAO) - Testimony Before the Subcommittees on Investigations and Oversight and Research and Technology Committee on Science, Space, and Technology House of Representatives, Statement of Candice N. Wright, Director, Science, Technology Assessment, and Analytics.

Number 6 (Page 28)

Regulating for better outcomes - next steps in consumer credit

Nisha Arora, Director of Consumer and Retail Policy, given at Westminster Business Forum.

Number 7 (Page 32)

Failures and near misses in insurance

Overview of recovery and resolution actions and cross-border issues

Number 8 (Page 36)

ESMA unveiled its workstreams for 2022. What made the cut?

Number 9 (Page 39)

New Android malware allows attackers to monitor all user activity on infected devices

Number 10 (Page 41)

Episode 50: The Photonicist

Number 1

Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative

Deputy Attorney General Lisa O. Monaco announced the launch of the department's *Civil Cyber-Fraud Initiative*, which will combine the department's expertise in civil fraud enforcement, government procurement and cybersecurity to combat new and emerging cyber threats to the security of sensitive information and critical systems.

"For too long, companies have chosen silence under the mistaken belief that it is less risky to hide a breach than to bring it forward and to report it," said Deputy Attorney General Monaco.

"Well that changes today. We are announcing today that we will use our civil enforcement tools to pursue companies, those who are government contractors who receive federal funds, when they fail to follow required cybersecurity standards — because we know that puts all of us at risk. This is a tool that we have to ensure that taxpayer dollars are used appropriately and guard the public fisc and public trust."

The creation of the Initiative, which will be led by the Civil Division's Commercial Litigation Branch, Fraud Section, is a direct result of the department's ongoing comprehensive cyber review, ordered by Deputy Attorney General Monaco this past May.

The review is aimed at developing actionable recommendations to enhance and expand the Justice Department's efforts against cyber threats.

Civil Cyber-Fraud Initiative Details

The Civil Cyber-Fraud Initiative will utilize the False Claims Act to pursue cybersecurity related fraud by government contractors and grant recipients.

The False Claims Act is the government's primary civil tool to redress false claims for federal funds and property involving government programs and operations.

The act includes a unique *whistleblower* provision, which allows private parties to assist the government in identifying and pursing fraudulent conduct and to share in any recovery and protects whistleblowers who bring these violations and failures from retaliation.

The initiative will hold accountable entities or individuals that put U.S. information or systems at risk by knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches.

The benefits of the initiative will include:

- Building broad resiliency against cybersecurity intrusions across the government, the public sector and key industry partners.

- Holding contractors and grantees to their commitments to protect government information and infrastructure.

- Supporting government experts' efforts to timely identify, create and publicize patches for vulnerabilities in commonly-used information technology products and services.

- Ensuring that companies that follow the rules and invest in meeting cybersecurity requirements are not at a competitive disadvantage.

- Reimbursing the government and the taxpayers for the losses incurred when companies fail to satisfy their cybersecurity obligations.

- Improving overall cybersecurity practices that will benefit the government, private users and the American public.

The department will work closely on the Initiative with other federal agencies, subject matter experts and its law enforcement partners throughout the government.

Report Cyber-Fraud

Tips and complaints from all sources about potential cyber-related fraud, waste, abuse and mismanagement can be reported by accessing the webpage of the Civil Division's Fraud Section, which can be found at: https://www.justice.gov/civil/report-fraud

Number 2

Building Climate Scenario Analysis on the Foundations of Economic Research

Governor Lael Brainard, at the 2021 Federal Reserve Stress Testing Research Conference, Federal Reserve Bank of Boston, Boston

I want to thank all of you for joining our research conference and the organizing committee for inviting me to share some thoughts on climate scenario analysis.

Economic analysis suggests that climate change could have profound consequences for the level, trend growth, and variability of economic activity over time and across regions and sectors.

Some of these effects could occur gradually, while others could occur relatively quickly in the presence of "tipping points." Policy, technology, and behavioral responses could similarly have material financial consequences.

Against this backdrop, the Federal Reserve is carefully considering the potential implications of climate-related risks for financial institutions and the financial system, with scenario analysis emerging as a potential key analytical tool for that purpose.

Climate change is projected to have profound effects on the economy and the financial system, and it is already inflicting damage.

The Sixth Assessment Report by the Intergovernmental Panel on Climate Change (IPCC) notes that "if global warming increases, some compound extreme events with low likelihood in [the] past and current climate will become more frequent, and there will be a higher likelihood that events with increased intensities, durations and/or spatial extents unprecedented in the observational record will occur."

We can already see the growing costs associated with the increasing frequency and severity of climate-related events. The total cost of U.S. weather and climate disasters over the last 5 full years exceeds $630 billion, which is a record.3 During this period, massive flooding in the Midwest has caused billions of dollars in damages to farms, homes, and businesses.

The California Department of Insurance has documented growing problems with the availability of fire insurance for homeowners, and the state legislature provided new protections for wildfire survivors.

Last year was the sixth consecutive year that the United States experienced ten or more billion-dollar weather and climate disasters.

And this summer, Hurricane Ida alone is estimated to have caused more than $30 billion in insurance losses.

The pandemic is a stark reminder that extreme events can materialize with little warning and trigger severe financial losses and market disruptions, and the IPCC Sixth Assessment Report is a reminder of the high uncertainty and potential costs associated with climate-related risks.

It will be important to systematically assess the resilience of large financial institutions and the broader financial system to climate-related risk scenarios.

Climate Scenario Analysis

As we are learning from the pandemic, risks emanating from outside the economy can have devastating financial consequences.

As part of our prudential and financial stability responsibilities, we are developing scenario analysis to model the possible financial risks associated with climate change and assess the resilience of individual financial institutions and the financial system to these risks.

The future financial and economic consequences of climate change will depend on the severity of the physical effects and the nature and speed of the transition to a sustainable economy.

So it is important to model the transition risks arising from changes in policies, technology, and consumer and investor behavior and the physical risks of damages caused by an increase in the frequency and severity of climate-related events as well as chronic changes, such as rising temperatures and sea levels.

From the IPCC's work, we know that the physical risks related to climate change will grow over time, while the transition risks will depend in part on how abruptly policy, technology, and behavioral changes take place.

Since financial markets are forward looking, a change in expectations regarding climate-related risks could lead to a sharp repricing of assets at

any time. Acute hazards, such as damaging hurricanes, or climate-related policy changes could quickly alter perceptions of future risk or reveal new information about the value of assets.

Sudden asset price changes can lead to financial instability when they interact with other vulnerabilities, such as high leverage or correlated exposures.

Scenario analysis is a useful tool in assessing the links between climate-related risks and economic outcomes because it requires assessing the implications for financial stability and individual financial institutions in a systematic way.

The interactions across institutions and market segments must be traced out, and missing data must be identified, acquired, and analyzed, leading to a clearer picture of the transmission of risks.

Scenario analysis should ultimately facilitate estimating the possible effects on individual financial institutions as well as on financial markets more broadly.

By systematically modeling the effects of climate-related risks across the financial system, scenario analysis can help inform risk management at the level of individual financial institutions and more broadly.

Given that this conference is about stress testing, it is worth revisiting some lessons from the first generation of bank stress tests.

Bank stress tests were developed at the height of the 2007–09 financial crisis to provide a more systematic way to assess the effects of complex and interrelated exposures within the financial system.

The first test, known as the Supervisory Capital Assessment Program (SCAP), used simplified models with limited data inputs. Despite substantial uncertainty about the economy's path, the SCAP was broadly viewed as successful. It provided a solid foundation for building out the stress-testing program over the subsequent decade.

The stress test infrastructure and granular models and data that are currently available bear little resemblance to that first stress test.

In parallel, banks have improved their risk-management operations, and large banks now routinely use their own stress tests to assess and manage their risks.

So what are the lessons for scenario analysis? Starting down the path of climate scenario analysis, even with a rudimentary first attempt, will help with risk identification and suggest useful lessons to inform subsequent improvements in modeling, data, and financial disclosures.

Although we should be humble about what the first generation of climate scenario analysis is likely to deliver, the challenges we face should not deter us from building the foundations now.

To read more:
https://www.federalreserve.gov/newsevents/speech/brainard20211007a.htm

Number 3

Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements

Progress Report on the implementation of the FSB High-Level Recommendations

FSB FINANCIAL STABILITY BOARD

Executive summary

This report provides a status update on progress made on the implementation of the FSB high-level recommendations for Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements.

It discusses key market and regulatory developments since the publication of the FSB high-level recommendations in October 2020; takes stock of the implementation of the FSB high-level recommendations across jurisdictions; describes the status of the review of the existing standard-setting body (SSB) frameworks, standards, guidelines and principles in light of the FSB high-level recommendations; and identifies areas for consideration of potential further international work.

While the current generation so-called stablecoins are not being used for mainstream payments on a significant scale, vulnerabilities in this space have continued to grow over the course of 2020-21.

At present, stablecoins are being used primarily as bridge between traditional fiat currencies and other crypto-assets, which in turn are primarily held and traded for speculative purposes.

Increased participation by retail investors could give rise to broader financial stability issues through an erosion of trust in the financial system.

In the event that a stablecoin does enter the mainstream of the financial system as a means of payment and/or a store of value in multiple jurisdictions, with the potential to achieve substantial volume, it could become a global stablecoin (GSC).

The emergence of GSCs would pose greater risks to financial stability than existing stablecoins and may challenge the comprehensiveness and effectiveness of existing regulatory, supervisory and oversight approaches.

Ensuring appropriate regulation, supervision and oversight across sectors and jurisdictions will therefore be necessary to prevent any potential gaps and avoid regulatory arbitrage.

Overall, the implementation of the FSB high-level recommendations across jurisdictions is still at an early stage.

In the first half of 2021, the FSB conducted a comprehensive stock-take of the implementation of the FSB high-level recommendations on the regulation, supervision, and oversight of so-called “global stablecoin” arrangements of October 2020.

48 jurisdictions in the FSB and its Regional Consultative Groups (RCGs) participated in the stock-take covering 21 advanced economies and 27 emerging markets and developing economies.

Several jurisdictions have been reviewing and updating their legal and regulatory regimes to address specific risks arising from the emergence of stablecoins.

Jurisdictions have taken or are considering different approaches towards implementing the high-level recommendations.

As the stablecoin landscape is evolving rapidly and as regulatory and supervisory policies are being developed, the differences among regulatory approaches and classifications could be increasing.

For example, certain jurisdictions are seeking to implement the recommendations through the adoption of new rules and regulations, while others have amended or plan to amend existing rules and regulations in such a way that these are applicable to stablecoins.

Other jurisdictions have relied largely on existing regulatory, supervisory and oversight regimes to address the risks associated with stablecoins or with entities that are part of the stablecoin arrangement.

Differing regulatory classifications and approaches to stablecoins at jurisdictional level could give rise to the risk of regulatory arbitrage and harmful market fragmentation.

Standard-setting bodies are continuing to assess whether and how existing international standards may apply to stablecoin arrangements and, where appropriate, adjust their standards in light of the FSB high-level recommendations.

However, a number of issues may not be fully covered by ongoing work.

Authorities should rely on existing standards and principles relevant to the supervision and oversight of GSC arrangements, where they perform the

same economic function as existing regulated activities covered by these standards. Any gaps in existing standards and principles should be addressed holistically and in a manner that is coordinated across sectors.

The FSB high-level recommendations complement the international standards and principles and should inform any potential updates to international sectoral standards and principles.

As jurisdictions are using the FSB high-level recommendations in developing their own domestic regulatory approaches, authorities have identified several issues relating to the implementation of the recommendations that may warrant further consideration and where further work at international level could be useful.

Areas for further consideration that respondents to the stock-take identified as most useful include conditions for qualifying a stablecoin as a GSC; prudential, investor protection, and other requirements for issuers, custodians, and providers of other GSC functions (e.g., wallet providers); redemption rights; cross-border and cross-sectoral cooperation and coordination; and mutual recognition and deference.

Further work on these issues at international level may help to support the effective implementation of the FSB high-level recommendations at the jurisdictional level, to mitigate the risk of regulatory fragmentation and arbitrage, and to address risks to financial stability arising from GSCs.

Efforts by standard-setting bodies to review, and where appropriate adjust their standards can further promote international consistency and reduce the risk of arbitrage or regulatory underlaps.

The work on fostering the soundness of GSCs is an integral part of the Roadmap for enhancing cross-border payments endorsed by the G20 in October 2020.

The Roadmap, which the FSB has developed in coordination with relevant international organisations and SSBs, calls for a review by the FSB, to be undertaken in consultation with other relevant SSBs and international organisations, of the FSB high-level recommendations.

This progress report and the underlying stock-takes, as well as ongoing and planned work from SSBs, will inform that review.

The FSB will continue to support the effective implementation of the FSB high-level recommendations and facilitate coordination among SSBs.

Starting in January 2022, with an expected completion date of July 2023, the FSB will review, in consultation with other relevant SSBs and international organisations, the recommendations in the FSB report and how any gaps identified could be addressed by existing frameworks.

The FSB will update its recommendations, if needed.

To read more: https://www.fsb.org/wp-content/uploads/P071021.pdf

Number 4

PLI Broker/Dealer Regulation and Enforcement 2021

Gurbir Grewal, Director, Division of Enforcement, Washington D.C.

Thank you for that introduction and for having me here today. At the Division of Enforcement, ensuring that broker-dealers and associated individuals follow our laws and regulations is critical to our mission, so it's only fitting that my first speech as Director is at this event.

While I just referred to it as "our mission" at the Division of Enforcement, what I'd like to talk to you about today is how we all share the responsibility to maintain market integrity and enhance public confidence in our securities markets. But first I must provide the disclaimer that my remarks today express my views, and do not necessarily reflect those of the Commission, the Commissioners, or other members of staff.

- SEC Charges Broker Who Defrauded Seniors Out of Almost $1 Million

- SEC Charges Ernst & Young, Three Audit Partners, and Former Public Company CAO with Audit Independence Misconduct

- SEC Charges Disbarred New York Attorney and Florida Attorney with Scheme to Create False Opinion Letters

- Merrill Lynch Admits to Misleading Customers about Trading Venues

- SEC Charges U.S. Congressman and Others With Insider Trading

These are not headlines from some bygone era of market participants behaving badly; these are all from cases the Commission has brought since 2018. In fact, here's one from just last week: "SEC Charges Investment Bank Compliance Analyst with Insider Trading in Parents' Accounts."

Nearly a dozen years ago, one of my predecessors held a press conference to announce charges against more than twenty defendants, including "Wall Street professionals, corporate insiders, analysts and lawyers," in a pair of alleged insider trading schemes.

In explaining the importance of the cases, Director Khuzami said: "There is a basic principle that governs our capital markets, and that is that there is one set of rules, and everyone is expected to play by that one set of rules. That principle gives investors confidence that the markets are fair."

He was right then, and his words remain true today: Enforcement is, in significant part, animated by the idea that we will pursue potential violations by any market participant, and, in so doing, attempt to shape the behavior of all participants going forward.

But I believe more is required. Because despite all of the strong enforcement actions the SEC has brought over the years and despite all the speeches that SEC Chairs, Commissioners, Enforcement Directors, and others have given at events like this one, the types of behavior described in the headlines I read to you persist, and as a result, a significant part of the public continues to feel that our markets are essentially a game that is rigged against them.

So rather than issue warnings about how aggressively we will pursue you or your clients if you misbehave—which we, of course, will—I want to invite each of you—the lawyers, counselors, and gatekeepers who have such influence over market behavior—to join me.

By working together, we can dispel the notion that the deck is stacked in favor of the few and powerful, promote better conduct among market participants, and ensure that the markets work fairly for all. This, after all, should be our shared mission.

I see three key steps towards achieving this mission, and the first starts with each of you. In a speech he gave in May, Chair Gensler said: "[I]f you're asking a lawyer, accountant, or adviser if something is over the line, maybe it is time to step back from the line. Remember that going right up to the edge of a rule or searching for some ambiguity in the text or a footnote may not be consistent with the law and its purpose." This is a critical point and let me explain why.

This morning you heard discussions on a number of topics, including SPACs, ESG investments, and Regulation Best Interest, or "Reg BI". I defer to your able presenters as to the best substantive takeaways from each of those sessions.

But what you should not take away from them is that, if regulators are particularly focused on issues "X" or "Y" in a given area, that means you or your clients may be able to push the envelope on issue "Z" – or the grey areas around X or Y. That approach is a surefire way to foster misconduct and, potentially, lead to an enforcement action.

You should be thinking, instead, about modeling excellence in your compliance efforts, as you do in your performance. This means that firms need to think rigorously about how their specific business models and

products interact with both emerging risks and Enforcement priorities, and tailor their compliance practices and policies accordingly.

For example, with respect to Reg BI, firms should recognize that the new regime draws upon key fiduciary principles, and is intended to enhance previous broker-dealer standards of conduct significantly beyond the suitability obligation.

Armed with this recognition, firms should then give their registered representatives the tools and information that will enable them to identify, disclose, and mitigate conflicts prohibited under Reg BI.

Let me be clear here: I am talking about more than putting together a stock policy and giving a check-the-box training. This requires proactive compliance, and this type of approach has never been more important than today— a time of rapid and profound technological change.

This change is exciting; it can help amplify the dynamism of our markets and increase access for investors. But at the same time it also creates new avenues for misconduct, and new responsibilities for compliance.

Recordkeeping violations may not grab the headlines, but the underlying obligations are essential to market integrity and enforcement. Take for example an enforcement action the Commission brought last year against a California broker-dealer for failing to preserve business-related text messages.

The SEC's order found that some of the firm's registered representatives used their personal devices when communicating with each other, with firm customers, and with other third parties concerning, among other things, the size of orders, the timing of trades, and the pricing of certain securities. These messages were potentially responsive to a records request SEC staff made to the firm in an unrelated investigation and the firm's failure to retain and produce them directly impacted that investigation.

Unfortunately, this is not an isolated example. We continue to see in multiple investigations instances where one party or firm that used off-channel communications has preserved and produced them, while the other has not. Not only do these failures delay and obstruct investigations, they raise broader accountability, integrity and spoliation issues.

A proactive compliance approach requires market participants to not wait for an enforcement action to put in place appropriate policies and procedures to preserve these communications and anticipate these emerging challenges.

Listen, many of these are not even new technological advances. After all, my 75 year-old mother has been texting my 13-year-old daughter for years, and I am certain many in this room have sent or received professional communications on personal devices or unofficial communications channels.

You need to be actively thinking about and addressing the many compliance issues raised by the increased use of personal devices, new communications channels, and other technological developments like ephemeral apps.

Let me turn to the second part of our shared mission, which I'll call proactive enforcement. While this falls primarily on us, each of you have a role to play here as well.

I'm from Jersey, and I know a thing or two about the Turnpike, and the Garden State Parkway, and about enforcement of my State's laws, having served as a County Prosecutor and as Attorney General.

And one thing I know is that if you post a 65 mile-per-hour speed limit and don't enforce it, people drive 75. Not me, of course, but other people. And they eventually do so with a sense of impunity. And then after a while they will drive 80 or faster, with a growing sense of confidence.

As speeds climb higher and higher, you eventually have situations where accidents increase and heightened enforcement follows. But for all of the victims, it's too late.

It's a stark analogy, but the point is that we are not waiting for accidents to happen. We are trying to address emerging risks before they cause harm to investors. For example, this summer, the Commission brought enforcement actions against a SPAC, its sponsor, its CEO, the proposed merger target, and the target's founder and former CEO.

The SEC's settled order against everyone but the target's CEO found that the target had made misleading claims about its technology and about national security risks associated with its founder and former CEO, and that the SPAC had repeated those misstatements in public filings and failed its due diligence obligations to investors. By bringing this action prior to consummation of the merger, the Commission protected the SPAC's investors from potential harm.

A similarly forward-looking enforcement initiative this past summer involved the new requirement that firms file and deliver Client or Customer Relationship Summaries, known as "Forms CRS." A Form CRS is designed

to help retail investors better understand the nature of their relationships with financial firms and individual professionals.

In July, the Commission brought enforcement actions against more than two dozen firms that had failed to timely file or to deliver their Forms CRS to their clients and customers.

As I said when we announced these cases, they "reinforce the importance of meeting [filing and disclosure] obligations and providing retail investors with information that is intended to help them understand their relationships with their securities industry professionals."

Providing retail investors that essential information is the point of the Form CRS requirement, and we will continue to ensure that firms are satisfying their obligations to do so because that's what's required to prevent future investor harm.

You also have a key role to play in spotting and addressing emerging risks, and that's both by ensuring that your proactive compliance efforts continue even after violative conduct has occurred and by working with us in addressing that conduct. Firms' cooperation with our investigations, including through voluntary self-reporting of potential violations, benefits all market participants.

Over the last several months, I have heard time and again that we are insufficiently clear regarding our views on cooperation. So let me try and offer some clarity. First, let me be clear about what cooperation is not: cooperation is not the mere absence of obstruction.

We do not recommend that parties receive credit for simply living up to their legal and regulatory obligations. Cooperation—at least the sort of cooperation that results in credit—means more than responding to lawful subpoenas.

It means more than making witnesses available for lawfully-compelled testimony. Any defense counsel who advises that credit may be on the table for taking these standard steps is doing their client a disservice.

Cooperation also means more than "self-reporting" to the SEC only when your violation is about to be publicly announced through charges by another regulator or an article in the news media.

And it certainly means more than conducting a purportedly independent investigation and making a presentation to the staff that does not fairly present the facts, but instead is nothing more than an advocacy piece.

The behaviors that can earn cooperation credit are no secret: the Seaboard Report turns 20 years old this month; the SEC's Policy Statement Concerning Cooperation by Individuals was issued in 2010; and the Enforcement Manual includes pages of discussion concerning the relevant tools and analytical frameworks.

And in several recent orders, the Commission has described the kinds of behavior that can garner cooperation credit.

For example, last September, the Commission charged BMW for disclosing inaccurate and misleading sales numbers in connection with a bond offering.

The SEC's order detailed the many steps BMW took during the global pandemic to collect, synthesize, translate where necessary, and present significant volumes of relevant materials to staff.

The order highlighted how "BMW also made multiple current and former employees available for interviews by the Staff, and provided presentations and narrative submissions that highlighted critical facts."

In short, BMW's cooperation "substantially advanced the quality and efficiency of the Staff's investigation and conserved Commission resources," and this was reflected in the Commission's decision to impose a reduced penalty against BMW.

But in case it's helpful, let me also tell you how I specifically think about cooperation. I look to whether the would-be cooperator took significant, tangible steps that enhanced the quality of our investigation, allowed us to conserve resources and bring charges more quickly, or helped us to identify additional conduct or other violators that contributed to the wrongdoing. If any or all of these occurred, then credit may be appropriate.

One last thing on cooperation. If you think you deserve credit, and the staff disagrees, I encourage you take a hard, objective look at your conduct during the investigation before trying to convince me the staff is wrong.

As someone who has served as a federal prosecutor, local prosecutor, and state Attorney General, I firmly believe that frontline staff are best-positioned to assess cooperation with the investigations they conduct.

They know the record and they know whether you meaningfully benefited those investigations. I respect their experience and will not only seek their input on decisions, but will also generally defer to their expertise and judgment.

At the same time, I will not look favorably on attempts to make an end run around staff to present the same, undisputed facts about your conduct to me in hopes of a more sympathetic ear.

Similarly, you should understand that we have a close relationship with our colleagues in EXAMS. If a party or its counsel engage in dilatory or obstructive tactics in an examination that gives rise to a referral, I will take a dim view of arguments that you deserve credit for cooperation with the ensuing enforcement investigation. As I said earlier, a key consideration in weighing cooperation is whether it conserves Commission resources, and this goes for those of our colleagues across the Commission.

Finally, I want to discuss the third step in our shared mission. This one applies when the first two steps have not worked. In that scenario, all of our enforcement tools are on the table, including monetary penalties.

Penalties are among the most important of our tools, in part because of our ability to tailor them to the violation. When Congress granted the SEC penalty authority in the Remedies Act of 1990, one perceived benefit was the SEC's ability to more finely calibrate its enforcement remedies against regulated entities, including broker-dealers.

By granting penalty authority, the Remedies Act empowered the Commission to impose remedies that were substantially more punitive than a censure, but less draconian than revoking a firm's registration or suspending its operations, and thereby potentially harming its customers.

The factors that guide us as we tailor our penalty recommendations are also no secret—we assess the conduct at issue in light of elements including statutory tiers, Commission guidance and judicial opinions, and resolutions in Commission actions involving comparable facts, violations, and parties.

One crucial question we also try to answer is what penalty will appropriately deter future misconduct? After all, penalties calibrated to both the offense and the offender, serve two interlocking purposes: punishment of the wrongdoer and deterrence of future misconduct, both by the penalized party and by others in the market.

And central to deterrence is proportionality. The worse the conduct, the more strongly we want to disincentivize market participants from engaging in it. We must design penalties that actually deter and reduce violations, and are not seen as an acceptable cost of doing business.

What does this mean for our approach to penalties in enforcement actions? As Commissioner Crenshaw put it earlier this year: "[C]orporate penalties

should be tied to the egregiousness of the actual misconduct." I agree wholeheartedly. But this does not mean that roughly equivalent misconduct by comparable offenders should be penalized in the same amount the hundredth time it occurs as the first. Rather, to achieve the intended deterrent effect, it may be appropriate to impose more significant penalties for comparable behavior over time. Doing so will make it harder for market participants to simply "price in" the potential costs of a violation.

As we evaluate the relevant penalty factors, we will also be closely assessing whether prior penalties have been sufficient to generally deter the misconduct at issue.

Where they have not been, you can expect to see us seek larger penalties, both in settlement negotiations and, if necessary, in litigation. Even if a firm or individual hasn't offended before, if they violate a law or rule for which the SEC has previously and publicly charged other actors in their industry, it may be appropriate for penalties or other remedies to be increased in response to the lack of deterrence.

So while penalties levied in the past are certainly a relevant data point for our conversations, you should not expect comparable cases to be the beginning and end of our analysis.

Similarly, one factor that has long weighed in our penalty assessments is the recidivism of the specific offender.

When a firm repeatedly violates our laws or rules, they should expect to be penalized more harshly than a first-time offender might be for the same conduct. This is the essence of specific deterrence.

I am confident that by engaging in proactive compliance and meaningful cooperation, and, where necessary, imposing significant, but appropriate penalties, through our enforcement efforts, we will not only reinforce market integrity, but also enhance public confidence in our markets. I look forward to working with all of you in achieving this, our shared mission.

Number 5

Agency Actions Needed to Address Foreign Influence

US Government Accountability Office (GAO) - Testimony Before the Subcommittees on Investigations and Oversight and Research and Technology Committee on Science, Space, and Technology House of Representatives, Statement of Candice N. Wright, Director, Science, Technology Assessment, and Analytics.

What GAO Found

U.S. research may be subject to undue foreign influence in cases where a researcher has a foreign conflict of interest (COI).

Federal grant-making agencies such as the National Science Foundation (NSF) can address this threat through COI policies and requiring the disclosure of information that may indicate conflicts.

In a December 2020 report, GAO reviewed five agencies, including NSF, which together accounted for almost 90 percent of all federal research and development expenditures at universities in fiscal year 2018.

GAO found that three of the agencies it reviewed have agency-wide COI policies and two do not.

The three agencies with existing COI policies focus on financial interests and do not specifically address or define non-financial interests, which may include multiple professional appointments.

In the absence of agency-wide COI policies and definitions for non-financial interests, researchers may not fully understand what they need to report on their grant proposals, leaving agencies with incomplete information to assess the risk of foreign influence.

Elements of Conflict of Interest (COI) Policies at Selected Agencies

	National Science Foundation	National Institutes of Health	National Aeronautics and Space Administration	Department of Defense	Department of Energy
Agency-wide COI policy	✓	✓	✓	No Agency-wide COI Policy	
Addresses financial COI	✓	✓	✓		
Addresses non-financial COI	—	—	—		

Source: GAO analysis of agency documents. | GAO-22-105434

In the report, GAO found that agencies were working with the Office of Science and Technology Policy (OSTP) on efforts to protect federally funded research and were waiting for OSTP to issue guidance on addressing foreign influence before updating their policies.

In January 2021, the White House and OSTP issued documents for agencies and research organizations, respectively, on actions to strengthen protections for federally funded research against foreign influence.

As of September 2021, OSTP is working on implementation guidance for agencies, due to be issued in November 2021.

All five agencies have mechanisms to monitor and enforce COI policies and requirements. While most agencies collect non-financial information, such as details of foreign collaborations, agencies rely on universities to monitor financial conflicts.

All five agencies have enforcement mechanisms for responding to an alleged failure to disclose required information, however, only NSF and the National Institutes of Health have written procedures for such allegations.

In addition, agencies have referred cases for criminal investigation, among other enforcement actions, where they identified researchers who failed to disclose required information.

Chairman Foster, Chairwoman Stevens, Ranking Members Obernolte and Waltz, and Members of the Subcommittees:

Thank you for the opportunity to discuss our December 2020 report on foreign influence in federally funded research.

The federal government reportedly expended about $44.5 billion on university science and engineering research in fiscal year 2019.

Safeguarding U.S. taxpayers' investment in federally funded research from undue foreign influence is of critical importance.

Recent reports by GAO and others have noted challenges faced by the research community to combat undue foreign influence, while maintaining an open research environment that fosters collaboration, transparency, and the free exchange of ideas.

For example, we recently reported on the risk foreign students working at U.S. research universities may pose by transferring sensitive knowledge they gain to their home countries.

In August 2018, the Director of the National Institutes of Health (NIH) sent a letter to over 10,000 universities highlighting concerns over foreign government talent recruitment programs, noting that these programs can influence researchers receiving federal funding to divert intellectual property and federally funded research to other countries.

The letter also highlighted concerns that some researchers who receive federally funded grants did not disclose financial and other resources provided by foreign governments.

For example, in May 2020, a former researcher at one U.S. university pleaded guilty for not reporting hundreds of thousands of dollars in foreign income on his federal tax returns, in relation to his involvement in the Thousand Talents Program, a Chinese-government talent recruitment program.

This case came to light after the agency reviewed the researcher's grant proposals and became concerned that he had failed to disclose, among other things, foreign research activity.

My testimony today summarizes the findings in our December 2020 report on foreign influence in federally funded research.

Specifically, it discusses

(1) the extent to which selected agencies and universities have conflict of interest policies and disclosure requirements that address potential foreign influence,

(2) the extent to which selected agencies have mechanisms to monitor and enforce policies and requirements, and

(3) the views of selected stakeholders on how to better address foreign threats to federally funded research.

For the report, we reviewed relevant laws, regulations, federal guidance, conflict of interest policies and requirements, and interviewed agency officials, university officials, and researchers about agency and university conflict of interest policies and disclosure requirements.

For this testimony, we asked the agencies we reviewed to provide updates on any steps taken to address the recommendations in our December 2020 report, and updated the recommendation status of selected agency activities, as appropriate.

This testimony, as well as the report, focuses on the top five agencies with the largest amount of funding for federal research, and which together accounted for almost 90 percent of all federal research and development expenditures at universities in fiscal year 2018—the Department of Defense (DOD), the Department of Energy (DOE), the National Aeronautics and Space Administration (NASA), NIH, and the National Science Foundation (NSF).

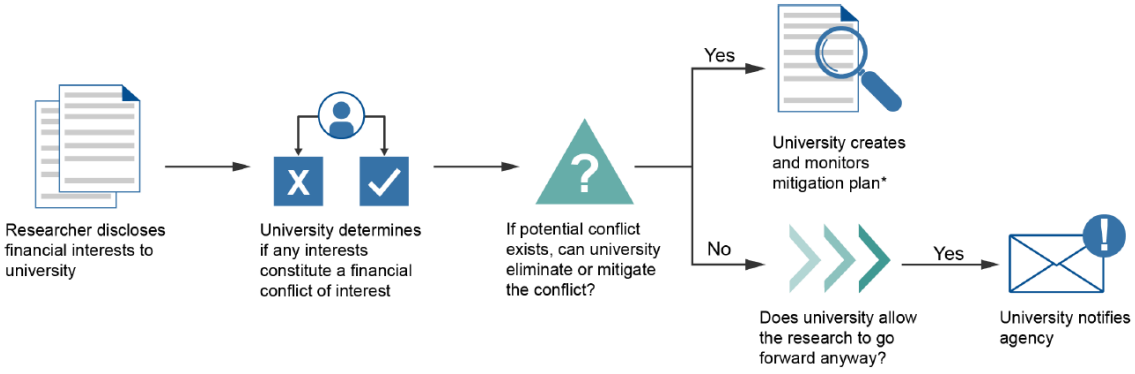
We also selected 11 universities, each of which received over $500 million in combined research grant funding in fiscal years 2018 and 2019 from two or more of the five selected agencies.

Additional information on our scope and methodology is available in our December 2020 report.

Our work was performed in accordance with generally accepted government auditing standards.

To read more: https://www.gao.gov/assets/gao-22-105434.pdf

Figure 1: Generalized University Processes for Identifying and Mitigating Potential Financial Conflicts of Interest



Source: GAO analysis of university and agency policies. | GAO-22-105434

*NIH regulations require universities to submit financial conflict of interest reports, including a description of the key elements of the university's mitigation plans. 42 C.F.R. § 50.605(b)(1)-(3). In addition, DOE officials told us that some of their components also require universities to submit mitigation plans. DOD noted that they may require such information in certain circumstances.

Number 6

Regulating for better outcomes - next steps in consumer credit

Nisha Arora, Director of Consumer and Retail Policy, given at Westminster Business Forum.

Highlights

- Consumer credit remains a key priority for the FCA as the consequences of the pandemic for consumers continue to unfold

- We are increasing our focus on consumer outcomes and needs, particularly for those in vulnerable circumstances; and bringing to bear the FCA's new, more innovative, more assertive and more adaptive approach

- We are consulting on a new Consumer Duty and working on new regulation for buy-now-pay-later products; we're also focusing on support for borrowers in financial difficulty and people who use high-cost credit products

- Credit is a huge and rapidly changing market - firms, consumer and debt advice organisations, government and the FCA need to continue to work together so that it delivers the right outcomes for consumers.

It's never been more important that the consumer credit market works well for consumers, firms and the economy. The consequences of coronavirus (Covid-19) are still unfolding, and we are yet to see what the "new normal" looks like.

Those consequences have been more severe for those in difficult financial circumstances, and millions more people now find themselves in that situation. Between February and October last year, 20 million adults in the UK saw their financial situation worsen, and nearly 10 million saw their unsecured debts increase.

Citizens Advice Bureaux in England and Wales took nearly 40% more calls about debt in August 2021 than they did in August 2020. You may visit: https://themoneycharity.org.uk/media/September-2021-Money-Statistics.pdf

Delivering better outcomes in consumer credit

Credit and debt affect the daily lives of tens of millions of people. That's why, as it has been since the FCA was formed, consumer credit remains one of our key priorities. Since the start of our regulation of credit markets, we have significantly improved outcomes for consumers using credit.

Our credit card remedies will save consumers up to £13 billion by 2030. We've better protected people in vulnerable circumstances, and we've secured more than £900 million in redress for those who have been poorly treated by credit firms.

And the response to the pandemic showed the FCA, the industry, and debt advice bodies at their best, working together to give consumers security and protection in the face of sudden instability and uncertainty.

But there is much more to do. And in a world where credit markets are changing rapidly, where we see innovative products and increasing digitalisation, and where consumer needs and demands are changing, the FCA needs to respond as a forward-looking and proactive regulator.

Our Chief Executive Nikhil Rathi has set out what this means in practice, and the three key shifts in the FCA's approach to regulation. We are becoming more innovative, using data and technology so that we can act more quickly and decisively.

We are becoming more assertive - making full use of our powers, helping others to use theirs, and playing our part in tackling issues that don't sit neatly within our regulatory perimeter. And we are becoming more adaptive, changing our approach more quickly as the world changes around us.

These shifts are essential to how we regulate credit markets and deliver the outcomes we want to see.

We want borrowers to have access to affordable products that meet their needs and don't lead them to become over-indebted; we want to see people being able to make informed decisions, and firms treating borrowers fairly – especially when they fall into difficulty. And we want to see firms competing vigorously and innovating to serve their customers better.

I'll talk now about our work to deliver these outcomes; much of which has been informed by the Woolard Review.

Underlying our approach to consumer protection and competition, across all retail markets, is an increased focus on consumer outcomes and needs, particularly for those in vulnerable circumstances.

When the pandemic began, we saw credit firms quickly and effectively adapting their processes and communications to deliver good outcomes for their customers. We want that to remain a focus for firms in credit and other markets, putting consumers at the heart of what they do.

And we want firms to take particular care with customers in vulnerable circumstances and at greater risk of harm, who may need more help to make decisions, or may be more susceptible to behavioural biases, or less able to manage debts.

Making firms focus on outcomes – a new Consumer Duty

Our focus on better consumer outcomes, particularly for the most vulnerable, runs through our vulnerability guidance and our proposals for a new Consumer Duty.

We see many good practices from credit firms, but we also see poor practices that hamper good decision-making, or that exploit behavioural biases and vulnerabilities.

That leads to products that are poor value or not fit for purpose, unacceptable customer service, and information that misleads consumers or fails to help them understand what they're signing up to.

As market offerings become more complex and digitalisation increases the speed of transactions, consumer decision-making becomes even harder.

We need to ensure our regulation adapts to the changing market environment.

When we think back to how different consumer credit was five or ten years ago, it underlines the importance of adaptive regulation that can respond and develop as the market does.

The proposed Consumer Duty will set the standards for firms in all retail markets including consumer credit. Firms will have to have a greater focus on consumer outcomes and act to enable these.

They will need to test what happens when consumers use their products and services – if credit products are causing financial harm or aren't delivering the right outcomes, firms will need to fix this.

Later this year, following our recent consultation, we plan to consult on proposed rules and set out our approach to supervision and enforcement under the new Duty.

That approach will be informed by our emphasis on being more innovative, adaptive and assertive – using data to allow us to intervene early as harm emerges, building flexibility into our approach so that we can address market changes, and acting quickly to improve and tackle poor practices before they become entrenched.

Regulation for unregulated buy-now-pay-later products

That emphasis will also inform our approach to buy-now-pay-later products that we don't currently regulate. We need to revisit the boundaries of what is and isn't regulated credit as new products develop and consumers' use of them changes.

As both the Woolard review and Nikhil have said, we need to take a holistic view of markets, acting assertively on harm around the edges of our regulatory perimeter, regulating according to what consumers need and use in the real world.

We agree with Chris Woolard that buy-now-pay-later is a product that can have important benefits for consumers as it develops and becomes more widespread, but it also carries risks and the potential for harm. We expect the Government to consult on a proposed regulatory framework in the next few weeks.

After that, we will follow with our own consultation on the relevant FCA rules, to set clear standards for firms. But we're certainly not sitting back and waiting. We are using existing powers to protect buy-now-pay-later users – for example, scrutinising marketing materials and the way these products are promoted. We have consumer protection powers outside of the Financial Services and Markets Act regime which we can apply to unauthorised firms where we see poor practice.

To read more:
https://www.fca.org.uk/news/speeches/regulating-for-better-outcomes

Number 7

Failures and near misses in insurance

Overview of recovery and resolution actions and cross-border issues

This is the second report on insurance failures and near misses by the European Insurance and Occupational Pensions Authority (EIOPA).

It aims at enhancing supervisory knowledge on the prevention and management of insurance failures, based on the information contained in the EIOPA database, which comprises a sample of 219 affected insurance undertakings in 31 European countries, dating back from 1999 to 2020.

The present paper strives to provide a better understanding of the kind of actions that are taken by insurers and NCAs when the companies are entering into two specific stages of the crisis management flow:

- i. The recovery phase (going-concern basis). This covers measures taken before the breach of the capital requirements (more specifically known

as preventive measures) and measures taken after the breach of the capital requirements.

- ii. The resolution phase (gone-concern basis). This phase refers to actions that taken by the authorities in charge of the resolution and/or liquidation process.

A number of additional issues such as potential policyholders' loss, external funding and crossborder aspects featuring insurers' failures and near misses are also studied here.

EIOPA commenced in 2014 to create a dynamic database of insurance failures and near misses. The objective was to gather relevant information from national competent authorities (NCAs) on relevant cases of insurance failures and near misses occurred in the European Economic Area (EEA), by means of gathering valuable information on the causes and early identification of insurance failures or near misses, as well as gauging their impact and the supervisory actions taken.

The first part of the current report is devoted to an analysis of the referred recovery and resolution actions adopted. Overall, the main findings suggest that the most common measures taken by the insurers and/or requested by the NCAs before and during the recovery phase, as documented in the EIOPA database, were:

- i. Presenting a recovery plan to restore compliance with the requirements; or (seldom) activating the existing pre-emptive recovery plan.

- ii. Requesting cash injections by shareholders or the parent company.

- iii. Require the reinforcement of internal governance arrangement and risk management.

- iv. Require commitment and/or actions from shareholders to support the company.

- v. Request additional provisioning (i.e. building up a higher level of technical provisions).

With regard to the resolution phase, the most common measures used by the NCAs were the following:

- i. Discontinue the writing of new business and continue administering the existing contractual policy obligations for in-force business (run-off),

- ii. Liquidation (i.e. the closure and orderly liquidation of the whole or part of a failing company),

- iii. Sale of all or part of the insurers' business to a private purchaser.

Policyholders in cases of insurance failures have not been immune to losses. Indeed, in the EIOPA's database, the policyholders in resolution suffered a loss of some kind in 30% of the cases.

Regarding the external funding (public funds or funds received by an Insurance Guarantee Scheme), the available evidence indicates that in 33% of the failures external injections were used.

When this was the case, the amount of external funds required to be injected or allotted to the insurer, was equal or higher than 20% of the total assets of such insurer in 47% of the cases.

Concerning the second part of the report, the analysis revolves around inspecting the most common issues arising on the resolution or liquidation of cross border insurance failures.

The continued increase of cross-border activity in insurance stresses the importance of a harmonised approach in protecting policyholders, especially considering the degree of internationalisation in the insurance sector.

The need to have in place an adequate system of policyholder protection appears clear in the event of cross-border insurance failures.

The available evidence show that the most common cross-border issue identified by the NCAs, in the cases of cross-border insurance failures, is related to the current fragmentation in the landscape of the national IGSs in the EU.

EIOPA has long argued that achieving a minimum degree of harmonisation in the field of IGSs is essential to provide a minimum level of protection to policyholders against the effects of an insurance failure.

Furthermore, due to the lack of harmonisation in the field of IGSs, there may be cases where an IGS is not able to neither cover nor compensate the losses of policyholders residing outside its own jurisdiction.

Depending on their place of residence and the geographical coverage, policyholders could be treated differently, which is an undesirable situation from the perspective of policyholder protection and internal market.

As documented in the second part of the report, there have not been many cross-border insurance failures reported yet (such as those insurers operating from abroad via freedom to provide services, FoS or freedom of establishment, FoE). However, the losses suffered by the policyholders in these cases seem to occur more often than in the cases of domestic insurance failures.

As a way to solve this it appears even more decisive now to have in the EU a recovery and resolution framework in place, as well as a minimum harmonised network of IGSs.

To read more:
https://www.eiopa.europa.eu/document-library/report/failures-and-near-misses-insurance_en

Number 8

ESMA unveiled its workstreams for 2022. What made the cut?

SPOTLIGHT ON MARKETS

Cloud outsourcing and financial stability risks

On 1 September, ESMA published its second Trends, Risks and Vulnerabilities (TRV) Report of 2021.

One of its in-depth articles analyses the growing use of cloud service providers (CSPs) by financial institutions and how the concentration of those providers can create financial stability risks in case of outage.

The analysis suggests that CSPs need to be significantly more resilient than firms to improve the safety of the financial system.

In financial settings where only longer outages cause systemic costs, the results suggest that CSPs can best address systemic risks by strongly reducing the time it takes to resolve incidents, rather than by reducing their frequency.

The analysis also shows that using a back-up CSP successfully mitigates the systemic risk caused by CSPs.

Increasing trend in the use of CSPs

While cloud computing is still a topic of research, it has become key to the digital economy.

Cloud computing is an innovation that allows for the use of an online network (the cloud) of hosting processors to increase the scale and flexibility of computing capacity.

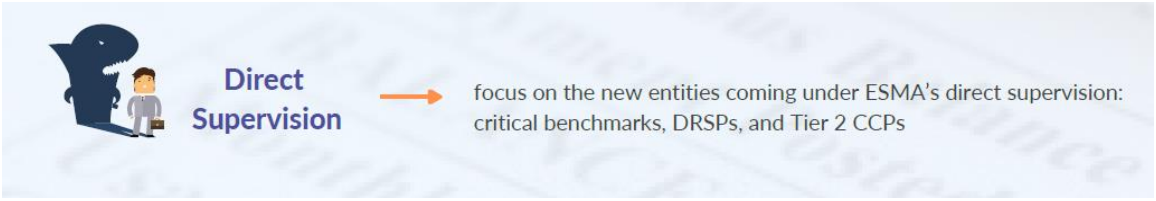
The use of cloud services by financial institutions has risen in recent years, as firms are increasingly outsourcing parts of their IT infrastructure.

The increasing trend has been further accelerated by the COVID-19 pandemic, as firms have had to set up remote working facilities.

There are many benefits associated with using cloud computing in the financial system. For example, cloud computing can lead to reductions in the cost of IT development and maintenance, increased flexibility and operational efficiency, enhanced information security.

In turn, this can increase the resilience of financial institutions, as they invest heavily in security and spread their infrastructures across geographical areas.

To read more:
https://www.esma.europa.eu/sites/default/files/library/newsletter_september_2021.pdf


Direct
Supervision
focus on the new entities coming under ESMA's direct supervision:
critical benchmarks, DRSPs, and Tier 2 CCPs

Number 9

New Android malware allows attackers to monitor all user activity on infected devices

National Cyber Security Centre

The malware, first seen last month in Canada and the US, has been named "Tanglebot" and allows attackers to gain access to all user activity via the *camera and microphone*, monitor the user's location and *steal any data* on the device, including messages and stored files.

The malware is spread via malicious text message, this is a form of phishing called smishing, which is an increasingly common method of spreading malware. Both phishing emails and smishing texts work by persuading victims to click on a link.

In this case, once the link is clicked "Tanglebot" victims are informed that Adobe Flash Player needs to be updated - Adobe stopped supporting Flash in December 2020 – and are led through a series of dialogue boxes which will allow the attackers to install and configure the malware. *Attackers then have full access to the device*.

The NCSC has published advice on how to deal with suspicious emails and messages such as this. You may visit:
https://www.ncsc.gov.uk/guidance/suspicious-email-actions

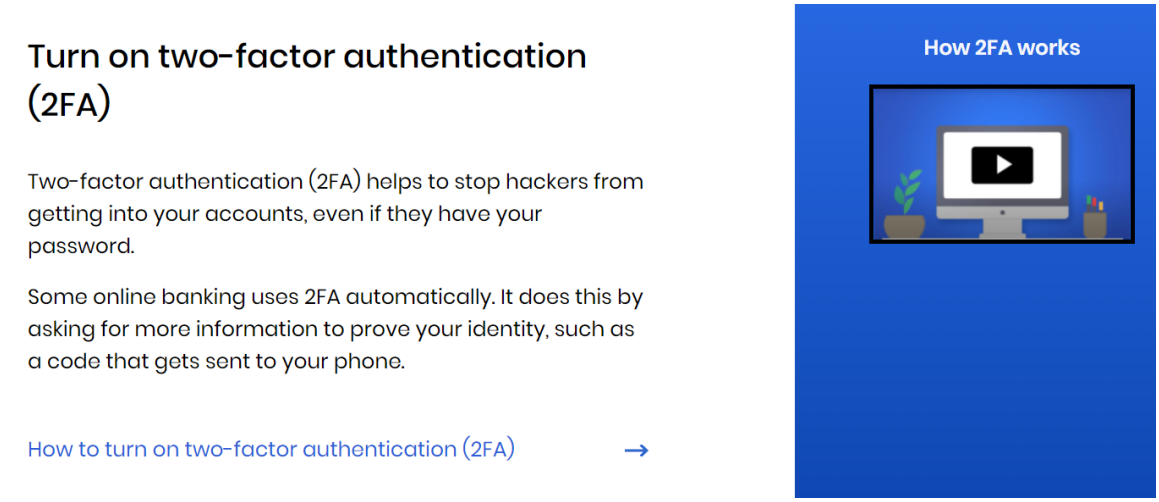
Spotting suspicious messages

Spotting scam messages and phone calls is becoming increasingly difficult. Many scams will even fool the experts. However, there are some tricks that criminals will use to try and get you to respond without thinking. Things to look out for are:

- **Authority** - Is the message claiming to be from someone official? For example, your bank, doctor, a solicitor, or a government department. Criminals often pretend to be important people or organisations to trick you into doing what they want.
- **Urgency** - Are you told you have a limited time to respond (such as 'within 24 hours' or 'immediately')? Criminals often threaten you with fines or other negative consequences.
- **Emotion** - Does the message make you panic, fearful, hopeful or curious? Criminals often use threatening language, make false claims of support, or tease you into wanting to find out more.
- **Scarcity** - Is the message offering something in short supply, like concert tickets, money or a cure for medical conditions? Fear of missing out on a good deal or opportunity can make you respond quickly.

Specifically, when receiving a scam text message, forward it to 7726. This free-of-charge short code enables your provider to investigate the origin of the text and take action, if found to be malicious.

The Cyber Aware website and our Individuals and Families page has additional advice to help you protect yourself online. You may visit: https://www.ncsc.gov.uk/cyberaware/home



Number 10

Episode 50: The Photonicist

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

In this episode of the Voices from DARPA podcast, Gordon Keeler, a program manager since 2017 in the agency's Microsystems Technology Office, takes listeners on a scenic tour of his efforts to integrate electrons and photons in ways that do more computing, more sensing, more decision-making, and more artificial intelligence in cheaper, smaller, lighter, and more energy-efficient packages than has been possible previously.

His work is a showcase of what technology insiders refer to as SWaP-C, which stands for Size, Weight and Power, and Cost.

Innovations that shrink one or all of those aspects of a technology can be far more important to realizing practical, affordable technologies and capabilities than the invention itself.

As Keeler explains how these and other technology drivers unfold in the half-dozen electronic, photonic, and optoelectronic programs he oversees, he also reveals what inspired him to give up the stable and secure job he held for 14 years before arriving at DARPA.

"I had no doubt really in my mind, DARPA clearly was the pinnacle of doing really innovative scientific research and development and leading the community to go do new things," Keeler tells listeners.

"I wanted to make an impact and DARPA was clearly a way to do that."

In that spirit, the Microsystems Technology Office will be running the 2021 ERI Summit, which from October 19-21 brings together leaders from across the electronics ecosystem to showcase technical achievements from

DARPA's five-year, $1.5B investment in the advancement of the U.S. semiconductor industry.

This year's Electronics Resurgence Initiative Summit will also celebrate MTO's 30th anniversary, recognizing the many contributions the office has made to the microsystems field throughout its history.

YouTube: https://youtu.be/8f5y1jD7_No

iTunes:
https://itunes.apple.com/us/podcast/voices-from-darpa/id1163190520

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.

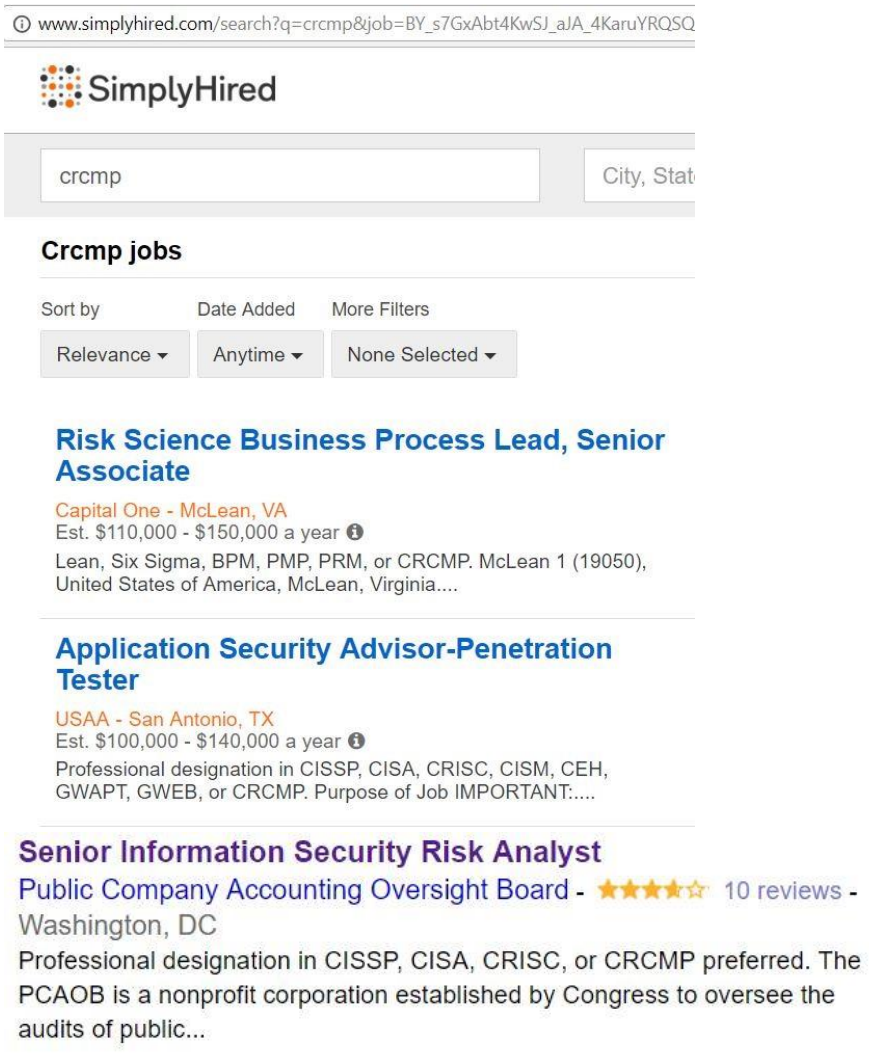
The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

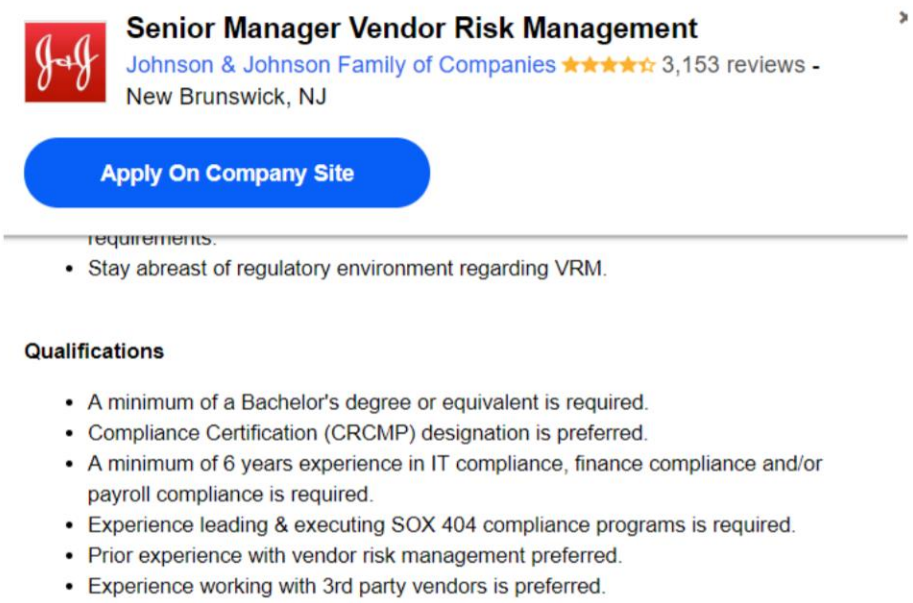
You can explore what we offer to our members:

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





Senior Manager Vendor Risk Management

Johnson & Johnson Family of Companies ★★★★☆ 3,153 reviews -
New Brunswick, NJ

Apply On Company Site

requirements.

- Stay abreast of regulatory environment regarding VRM.

Qualifications

- A minimum of a Bachelor's degree or equivalent is required.
- Compliance Certification (CRCMP) designation is preferred.
- A minimum of 6 years experience in IT compliance, finance compliance and/or payroll compliance is required.
- Experience leading & executing SOX 404 compliance programs is required.
- Prior experience with vendor risk management preferred.
- Experience working with 3rd party vendors is preferred.

Companies and organizations like Accenture, American Express, USAA etc. consider the Certified Risk and Compliance Management Professional (CRCMP) program a preferred certificate. There are CRCMPs in 32 countries.

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