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, March 22, 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,

Well, this paragraph raised my eyebrow. The title: *Risks arising from de-risking*.

De-risking refers to a decision taken by firms to refuse, or to terminate, business relationship with some categories of customers that they associate with higher money laundering and terrorism financing (ML/TF) risk.

This is part of the *Opinion of the European Banking Authority (EBA) on the risks of money laundering and terrorist financing affecting the European Union's financial sector*. The EBA notes that de-risking continues to pose ML/TF risks, because customers affected by de-risking may resort to alternative payment channels in the EU and elsewhere to meet their financial needs.

As a result, transactions may no longer be monitored, making the detection and reporting of suspicious transactions and, ultimately, the prevention of ML/TF more difficult.

Arthur Bloch, the author of the Murphy's Law books, has said that *every solution breeds new problems*. De-risking is a solution that breeds new ML/TF problems.

Arthur Bloch has also said that *friends come and go but enemies accumulate*. We must expect that ML/TF risks will accumulate too. We read in the document from the EBA that firms are more likely to de-risk corporate customers whose business involves processing significant volumes of cash transactions, or whose products allow for anonymity, such as anonymous pre-paid instruments or pre-paid instruments reloadable by cash or by *crypto-currencies*.

You can read more at number 3 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 7 (Page 22)

Exchange of Letters on Co-operation in the area of Insurance Supervision between the Financial Services Agency and the European Insurance and Occupational Pensions Authority

Number 8 (Page 26)

The future of capital is green

Ravi Menon, Managing Director of the Monetary Authority of Singapore, at IMAS-Bloomberg Investment Conference.

Number 9 (Page 27)

Who Can Find My Devices? Security and Privacy of Apple's Crowd-Sourced Bluetooth Location Tracking System

Alexander Heinrich, Milan Stute, Tim Kornhuber, and Matthias Hollick

Number 10 (Page 28)

Cyber-attack on the European Banking Authority

Number 1

2020 Annual Report

Large Bank Supervision

For state nonmember banks with assets exceeding $10 billion, the FDIC generally employs a continuous risk management examination program, whereby dedicated staff conduct targeted examinations and ongoing institution monitoring based on a comprehensive annual supervisory planning process.

Consumer protection and CRA examinations are generally conducted on a point-intime basis, although DCP initiated a pilot program during 2020 to employ a continuous supervision model.

The Large Insured Depository Institution (LIDI) Program remains the primary instrument for off-site monitoring of these institutions.

The LIDI Program provides a comprehensive process to standardize data capture and reporting for large and complex institutions nationwide, allowing for quantitative and qualitative risk analysis.

The LIDI Program focuses on institutions' potential vulnerabilities to asset, funding, and operational stresses, and supports effective large bank supervision by using individual institution information to focus resources on higher-risk areas, determine the need for supervisory action, and support insurance assessments and resolution planning.

In 2020, the LIDI Program covered 106 institutions with total assets of $3.7 trillion.

The Shared National Credit (SNC) Program is an interagency initiative administered jointly by the FDIC, OCC, and FRB to promote consistency in the regulatory review of large, syndicated credits, as well as to identify risk in this market, which comprises a large volume of domestic commercial lending.

In 2020, outstanding credit commitments in the SNC Program totaled over $5 trillion.

The FDIC, FRB, and OCC report the results of their review in an annual joint public statement.

Information Technology and Cybersecurity

The FDIC examines information technology (IT) risk management practices, including cybersecurity, at each bank it supervises as part of the risk management examination.

Examiners assign an IT rating using the FFIEC Uniform Rating System for Information Technology (URSIT).

The IT rating is incorporated into the management component of the CAMELS rating, in accordance with the FFIEC Uniform Financial Institutions Rating System.

During 2020, the FDIC conducted 1,319 IT examinations at state nonmember institutions, issuing 24 enforcement actions.

The FDIC also examines the services provided to institutions by bank service providers.

In addition to routine examination procedures, this year the FDIC, FRB, and OCC horizontally reviewed services provided by a sample of service providers to understand system capabilities for a potential zero interest rate environment, to assess readiness for the transition from LIBOR as the standard reference rate, and to obtain a high-level understanding of their ability to manage applicable aspects of the CARES Act.

To read more:
https://www.fdic.gov/about/financial-reports/reports/2020annualreport/2020ar-final.pdf

Number 2

Announcements on the end of LIBOR

The FCA has announced the dates that panel bank submissions for all LIBOR settings will cease, after which representative LIBOR rates will no longer be available.

This is an important step towards the end of LIBOR, and the Bank of England and FCA urge market participants to continue to take the necessary action to ensure they are ready.

The FCA has confirmed that all LIBOR settings will either cease to be provided by any administrator or no longer be representative:

- immediately after 31 December 2021, in the case of all sterling, euro, Swiss franc and Japanese yen settings, and the 1-week and 2-month US dollar settings; and

- immediately after 30 June 2023, in the case of the remaining US dollar settings

Based on undertakings received from the panel banks, the FCA does not expect that any LIBOR settings will become unrepresentative before the relevant dates set out above.

Representative LIBOR rates will not, however, be available beyond the dates set out above.

Publication of most of the LIBOR settings will cease immediately after these dates.

As ISDA has confirmed separately, the 'spread adjustments' to be used in its IBOR fallbacks will be fixed today as a result of the FCA's announcement, providing clarity on the future terms of the many derivative contracts which now incorporate these fallbacks.

The Bank of England and the FCA have made it clear over a number of years that the lack of an active underlying market makes LIBOR unsustainable, and unsuitable for the widespread reliance that had been placed upon it.

Accordingly, both have worked closely with market participants and regulatory authorities around the world to ensure that robust alternatives to LIBOR are available and that existing contracts can be transitioned onto these alternatives to safeguard financial stability and market integrity.

Market-led working groups and official sector bodies, including the Financial Stability Board, have set out clear timelines to help market participants plan a smooth transition in advance of LIBOR ceasing.

Today's announcements confirm the importance of those preparations for all users of LIBOR.

Regulated firms should expect further engagement from their supervisors at both the Prudential Regulation Authority and the FCA to ensure these timelines are met.

Authorities have also recognised that there are some existing LIBOR contracts which are particularly difficult to amend ahead of the LIBOR panels ceasing, often known as the 'tough legacy'. The FCA is taking steps to help reduce disruption in these cases.

The FCA will consult in Q2 on using proposed new powers that the government is legislating to grant to it under the Benchmarks Regulation (BMR) to require continued publication on a 'synthetic' basis for some sterling LIBOR settings and, for 1 additional year, some Japanese yen LIBOR settings.

It will also continue to consider the case for using these powers for some US dollar LIBOR settings.

Any 'synthetic' LIBOR will no longer be representative for the purposes of the BMR and is not for use in new contracts. It is intended for use in tough legacy contracts only.

The FCA will also consult in Q2 on which legacy contracts will be permitted to use any 'synthetic' LIBOR rate.

The FCA has also published today statements of policy in relation to some of these proposed new BMR powers.

These statements of policy confirm its policy approach, explain its plans set out above and its intention to propose using, as a methodology for any 'synthetic rate', a forward-looking term rate version of the relevant risk-free rate plus a fixed spread aligned with the spreads in ISDA's IBOR fallbacks.

FCA CEO Nikhil Rathi said:

'Today's announcements provide certainty on when the LIBOR panels will end. Publication of most of the LIBOR benchmarks will cease at the same time as the panels end. Market participants must now complete their transition plans.'

Bank of England Governor Andrew Bailey said:

'Today's announcements mark the final chapter in the process that began in 2017, to remove reliance on unsustainable LIBOR rates and build a more robust foundation for the financial system. With limited time remaining, my message to firms is clear – act now and complete your transition by the end of 2021.'

You can see the FCA's announcement regarding the future cessation and loss of representativeness of the LIBOR benchmark settings at: https://www.fca.org.uk/publication/documents/future-cessation-loss-representativeness-libor-benchmarks.pdf

Number 3

Opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the European Union's financial sector

Introduction and legal basis

1. Article 6(5) of Directive (EU) 2015/849 requires the EBA to issue an Opinion on the risks of money laundering and terrorist financing (ML/TF) affecting the European Union's financial sector *every two years*.

2. This is the third Opinion on the risks of ML/TF affecting the European Union's financial sector.

The EBA is issuing this Opinion as part of its new mandate to lead, coordinate and monitor the fight against ML/TF in the financial system at the EU level.

The European Securities and Markets Authority (ESMA) and European Insurance and Occupational Pensions Authority (EIOPA) were closely involved in the process.

3. The Opinion draws on information provided by competent authorities (CAs) and on information obtained in the context of the EBAs' work, such as the attendance at AML/CFT colleges and the EBA's AML/CFT implementation reviews.

4. As in its previous Opinion, the EBA looked at ML/TF risks to which credit and financial institutions are exposed, as well as ML/TF risks that cut across various sectors.

The EBA also carried out an assessment of how the ML/TF risks have evolved since the last Opinion was published in 2019.

5. This Opinion sets out proposed actions addressed to CAs, which are based on the detailed analysis and findings set out in the report annexed to the Opinion. The Opinion together with the report also serves to provide information for the European Commission's Supranational Risk Assessment (SNRA) and risk assessments carried out by CAs.

6. The EBA competence to deliver an Opinion is based on Article 29(1)(a) of Regulation (EU) No 1093/2010 and on Article 6(5) of Directive (EU) 2015/849 and Article 16a(1) 29(1)(a) of Regulation (EU) No 1093/2010, as risks of ML/TF affecting the European Union's financial sector relate to the EBA's area of competence.

7. In accordance with Article 14(7) of the Rules of Procedure of the Board of Supervisors, the Board of Supervisors has adopted this Opinion.

8. Under Article 29(1)(a), the EBA has, where appropriate, to conduct open public consultations and a cost-benefit analysis (CBA) and request advice from the Banking Stakeholder Group (BSG).

Consultation/CBA must be proportionate to the scope, nature and impact of the Opinion. In this instance, the EBA has not conducted an open public consultation and CBA and has not requested advice from the BSG because the suggestions made to CAs in this Opinion do not change or specify policies, but rather set out good practices and reiterate supervisory duties.

In relation to the proposals addressed to the national competent authorities, they would mainly impact the authorities that have already contributed to the development of this Opinion, and so there was no need to seek their views through an open public consultation.

To read more:
https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2021/963685/Opinion%20on%20MLTF%20risks.pdf

Number 4

BIS Bulletin No 38, Covid-19 bank dividend payout restrictions: effects and trade-offs

Bryan Hardy

Key takeaways

• In the context of the Covid crisis, authorities adopted dividend payout restrictions to enhance bank resilience and support stronger growth in bank lending. Restrictions may reduce short-term equity returns for bank shareholders, especially in the case of banks with a low price-to-book ratio.

• In line with these predictions, bank equity prices fell with dividend restriction announcements, but credit default swap (CDS) spreads indicated that default risk either fell or was unaffected, even in the face of the economic downturn.

• Bank capitalisation rose in jurisdictions which restricted payouts, supporting institutional and systemwide stability; the increased capital was more likely to support greater lending with restrictions present.

Covid-19 presents an ongoing challenge for supervisors and other policymakers charged with ensuring financial stability while maintaining the flow of credit to the economy.

To address these goals, regulators adopted a number of policy measures, including restrictions on bank capital payouts such as dividends.

Payout restrictions were intended to preserve bank capital in case large losses arose and channel bank resources towards lending.

This Bulletin examines how these restrictions affected banks' payouts, capitalisation and lending, and their effect on banks' equity prices and credit default swap (CDS) spreads.

Capital payouts by banks can set at odds the interests of different bank stakeholders, such as shareholders and creditors.
Bank valuations fell in March 2020 during the initial pandemic turmoil, driving incentives to pay dividends to boost short-term shareholder returns (Gambacorta et al (2020)).

However, such payouts erode the existing book capital base and increase riskiness, contrary to the interests of debt investors and depositors.

They also reduce the capital available to support lending, with negative implications for borrowers and the broader economy.

For these reasons, dividend restrictions did not receive unqualified support from all stakeholders. And a number of additional considerations qualify the crisis-time trade-offs outlined above (ESRB (2020)).

Retaining more capital can lower borrowing costs for banks, but it could also discourage future efforts to raise equity.

A sector-wide ban on payouts can remove the stigma for those individual banks that restrict dividends, but it punishes prudent banks with sizeable capital buffers that could safely pay out their profits.

This note sheds light on these arguments in the Covid-19 context, examining the evolution of banks' equity and CDS prices, and their capitalisation and lending around the implementation of payout restrictions.

Equity prices fell in tandem with the anticipated reduction in dividends, but CDS spreads did not rise. Capitalisation rose with restrictions, and such restrictions helped banks better leverage additional capital into more lending.

To learn more: https://www.bis.org/publ/bisbull38.pdf

Number 5

Dangerous Malware Dropper Found in 9 Utility Apps on Google's Play Store

Highlights

- Check Point Research discovered a new dropper being spread via 9 malicious Android apps on the official Google Play store

- The malware family allows the attacker to obtain access to victims' financial accounts and take full control of their mobile phone

- Google removed the apps from the Play store after being notified by Check Point Software

Our Findings

Check Point Research (CPR) recently discovered a new dropper spreading via the Google Play store. The dropper, dubbed Clast82, has the ability to avoid detection by Google Play Protect, complete the evaluation period successfully, and change the payload dropped from a non-malicious payload to the AlienBot Banker and MRAT.

To read more:
https://blog.checkpoint.com/2021/03/09/dangerous-malware-dropper-found-in-9-utility-apps-on-googles-play-store/

Number 6

Moving Forward Together – Enforcement for Everyone

SEC Commissioner Caroline A. Crenshaw

I want to thank the Council of Institutional Investors for inviting me today. You are tireless advocates for investors and staunch proponents of good corporate governance. The agenda for this year's meeting covers a number of timely topics that are top of mind for me as well – from the impact of COVID-19 on members, to drivers behind the SPAC boom, to diversity and inclusion at U.S. companies.

I'm pleased you are also talking about sustainable finance, proxy voting issues and ESG ratings. Further, I share CII's prioritization of clawbacks and transparency as to executive pay, stock trades and share buybacks. Today I have been asked to speak about what's next for the SEC. Before I do that, I will make the usual disclaimer that the views I express today are my own, and do not necessarily reflect those of staff, my fellow commissioners, or the agency.

In thinking about what I wanted to discuss today, of course I considered policy matters that I would like to see the Commission prioritize in the near term: Regulation Best Interest, the improvements needed in the proxy process, the need to finish implementing Dodd-Frank, and continuing updates to our market infrastructure. But I kept coming back to something even more foundational: our enforcement program.

I want to talk about the central role enforcement plays in fulfilling our mission, how investors and markets benefit, and how a decision made 15 years ago has taken us off course. And I'll explain how changing tack now will yield better outcomes in all these areas.

Over the years, Commissioners on both sides of the political aisle have agreed that a strong enforcement program incentivizes compliance with the securities laws, and that enforcement helps to promote a market that inspires investor confidence, creating a level playing field for market participants. But Commissioners have had different views about when corporate penalties further those goals.

It is clear to me that the Commission has historically placed too much emphasis on factors beyond the actual misconduct when imposing corporate penalties – including whether the corporation's shareholders benefited from the misconduct, or whether they will be harmed by the assessment of a penalty.

This approach is fundamentally flawed. This approach, more concerningly, could allow companies to profit from fraud as it unnecessarily limits the Commission's ability to craft appropriately tailored penalties that more effectively deter misconduct. If we are going to confront the novel issues today's markets present and deter ever more complicated and hard to detect frauds, we must revisit our approach.

This is a subject that I imagine matters to you as investors and market participants, because, unless there is a financial incentive to follow the rules, we know there is a temptation to break them. We know there is a temptation to spend money on operations at the expense of investing in compliance.

To help deal with those misaligned incentives, the Commission was given civil penalty authority, allowing it to tailor remedies to misconduct and effectively deter malfeasance to promote a fair market. Fairness yields better results for everyone. As CII members, you hold tremendous influence in the market and can help promote greater compliance with the securities laws, so I appreciate your time and attention today as I share my views.

In order to protect investors and promote our capital markets, we need not only dedicated staff and well-crafted regulations, but also for those regulations to be applied in a manner that promotes fairness.

This, in turn, will promote growth and success. And it is not a platitude; the last 90 years or so present a long-running event study that proves it. To a large extent, our current regulatory system emerged in direct reaction to abuses that were revealed following the stock market crash of 1929.

The '33 Act, and the legislation that followed, addressed weaknesses and failings of markets that had too long favored the rich and well-connected, who too often used their positions and advantages to treat retail investors as victims or marks, rather than owners.

The enactment of prudent regulation changed that dynamic, as did the creation of an enforcement regime that has evolved over time to better address violations.

The stability of our regulatory system has allowed our markets to prosper.

Many studies have confirmed that companies that play by the rules do better in the long-term, but only if their competition plays by the same rules.

It is unfortunate, but not surprising when companies fail to honor rules if they see competitors reaping (short-term) benefits by skirting them or outright cheating. Aggressive but even-handed enforcement, without fear or favor, protects law-abiding corporate citizens. It also incentivizes everyone to behave fairly and focus on operations rather than on racing to the bottom.

Against this backdrop, I have been, and will continue to be, focused on vigorous enforcement of our existing laws and regulations. As I'll explain further, enforcement best advances our agency's goals when it concentrates the costs of harm with the person or entity who committed the violation. For these reasons, ensuring that the violator pays the price is key to a successful enforcement regime and to promoting fair and efficient markets more broadly.

This "price" that I mention—the amount corporations have to pay when they violate the securities laws, has been a topic that the Commission and many commissioners have addressed over the years. In 2006, a unanimous, five-member Commission issued a statement discussing a multitude of factors that the Commission will consider when deciding whether to assess a penalty against a corporation.

In addition to stating that "corporate penalties are an essential part of an aggressive and comprehensive" enforcement program and contribute to the Commission's ability to deter misconduct, the 2006 statement suggested that the Commission should be careful not to impose penalties that unduly burden shareholders.

Since then, when assessing penalties, the Commission has looked at whether a corporation's shareholders benefited from misconduct, or whether they will be harmed by the assessment of a penalty because the costs may be passed on to shareholders. This myopic approach is flawed and the reason why we need to make a change.

First, corporate penalties should be tied to the egregiousness of the actual misconduct – not just the benefit or impact on the shareholders. It is common sense and bedrock to our law enforcement regime that worse conduct comes with stiffer penalties.

I agree with former Commissioner Luis Aguilar's observation that focusing on how and whether the penalty will impact the wrongdoer and its shareholders takes the focus off the actual misconduct at issue.

Even the unanimous 2006 statement acknowledged that corporate penalties must be tailored to the violation.

Second, the Commission should not treat the presence or absence of a shareholder or corporate benefit as a threshold issue to imposing a penalty. Let me explain. The rationale behind looking to whether a violation conferred an improper benefit on shareholders stems from the view that it is unfair to impose a penalty if shareholders will be harmed by that penalty, unless the shareholders also benefited from the violation.

While this rationale was the subject of many speeches following the release of the 2006 statement, time has revealed its limitations. Corporate benefit calculations are quite simply incomplete. This is because the shareholder benefit stemming from a violation is not limited to the assets the company acquired as a result of its violation, nor is it just the inflated stock price shareholders enjoyed. Corporate benefits include economic and intangible benefits that the company obtained when the market was in the dark about the full extent of the violation.

How do we identify and measure the benefits conferred by a good reputation, or determine the impact of dripping bad information out through multiple disclosures over time? How do we adequately measure the impact fraud has on the market? Does undisclosed fraud effectively reduce a company's capital costs?

And what if there is a stock buyback during the period the share price is inflated? Does that harm shareholders because the company is spending money to repurchase its stock, or does it actually further benefit them by potentially raising earnings per share (EPS)?

And one significant benefit we seem to have overlooked is the benefit all investors receive by encouraging companies to obey the law or face penalties.

If we are going to consider the benefit to shareholders, we need to consider all of the benefits. I disagree with the notion that a corporation should pay any less of a penalty simply because the total benefit it received from its misconduct is difficult to quantify with exact precision. If that were the case, corporations might actually profit from their fraud. That is a bad outcome and not what the securities laws were intended to achieve.

I want to say one additional thing about the shareholder harm concern. It is not clear to me that SEC penalties actually harm investors.

I am interested in seeing any and all data or studies on this point. If the penalties are sufficiently high to motivate the company to remediate problems, strengthen internal controls, clarify lines of responsibility, and prioritize individual accountability, those are all changes that likely lead to better future outcomes, and higher profits for shareholders.

Moreover, rarely do investors realize harms or gains by things that happen on a particular day, especially if they hold the shares for a period that exceeds the duration of the event's impact.

Finally, if we limit penalties to instances where shareholders benefited from the violation, then we're doing no more than disgorging the proceeds of corporate wrongdoing. Penalties are intended to incentivize compliance, and higher penalties can be effective in deterring violations that are particularly hard to detect.

There becomes less of an incentive for shareholders to invest in companies that choose to follow the law if there are no repercussions for investing in those that do not.

And for policy reasons, I think such an approach is likely to jeopardize the integrity of our capital markets in the long-term. Simply put, a single-minded focus on having companies pay a calculated corporate benefit will not appropriately deter fraud or ensure fair and efficient markets.

If our penalties were limited in such a way, the price of getting caught might not be high enough to deter misconduct.

So what should we do? In addition to gathering additional data that can better inform how we assess corporate penalties, we need to consider the impact of the other factors identified in the 2006 statement on penalties.

This, includes the degree to which a corporation self-reported its conduct, cooperated with law enforcement investigations, and then self-remediated violations.

Cooperation provides companies with a potential path toward reducing or, perhaps, entirely avoiding penalties because it promotes and protects investors' long-term interests.

Issuers should take note that the Commission takes cooperation and self-reporting seriously.

I want to make clear, however, that cooperation credit is not afforded to companies that merely respond to Enforcement Division requests, or to those that offer to conduct a not-so-independent investigation led by corporate counsel.

Meaningful cooperation requires a commitment to proactively identifying and remediating wrongdoing, as well as holding accountable those individuals responsible for misconduct.

It's about substantially shortening the staff's investigation and working with the staff toward an efficient resolution.

Additionally, because corporate benefits and shareholder harm are rather amorphous concepts, moving forward the Commission should focus on setting penalties that are based on the actual misconduct and reflect the extent of cooperation with the Division of Enforcement staff. We should consider the extent of harm to victims and, if we know it, the number of harmed investors.

Penalties should be higher for violations that cause more harm, either on their own or in the aggregate when considering their frequency. Similarly, we should also impose higher penalties on violations that are more difficult for us to detect. There is a greater need to deter conduct that requires more Commission resources to uncover, investigate and address.

The pervasiveness or complicity within the organization is another relevant consideration. Corporate culture comes from the top, and there is a strong need to incentivize companies to foster a culture of compliance – not misconduct. If companies believe they can profit from violations and are unlikely to be caught, they are more likely to break the rules.

We can help solve this by giving at least equal, if not even greater weight to the other factors mentioned in the 2006 statement.

That is how we will be most effective in deterring harmful misconduct – and we should remember that deterrence was a primary reason the Commission was given penalty authority in the first place.

The SEC has a three part mission, and protecting a company's shareholders is part of that, but not at the expense of the larger market, particularly when there are other companies – and shareholders – who have committed to and invested in compliance. So in setting penalties, we can't look only at

the impact the penalty will have on a particular group of investors who own shares in the specific violating entity. As the Commission noted 15 years ago, we must examine the impact more broadly.

We must think about the impact on all investors, and that will help ensure fair and efficient markets. Every enforcement decision we make effects multiple constituencies in myriad ways. Therefore, we must consider those impacts and seek the right balance. We must correct this course.

Thank you for your time and attention today and I look forward to your questions.

Number 7

Exchange of Letters on Co-operation in the area of Insurance Supervision between the Financial Services Agency and the European Insurance and Occupational Pensions Authority

Dear Mr Himino,

I believe that constructive dialogue and effective cooperation between the Financial Services Agency (FSA) and the European Insurance and Occupational Pensions Authority (EIOPA) with regards to strengthening the exchange of information on regulatory developments and enhancing the supervisory cooperation in relation to insurance companies would be mutually beneficial.

I also acknowledge that these steps are important in view of the globalisation of the insurance sector and the financial markets in which they operate.

In this context, this Exchange of Letters confirms our willingness to further enhance our regulatory and supervisory cooperation, in the interest of fulfilling our respective statutory objectives as further set out below in order to contribute to the protection of policyholders and to support the stability of the financial system.

The envisaged cooperation acknowledges the joint EU-Japan financial regulatory forum established under the Japan-EU Economic Partnership Agreement.

EIOPA and the FSA enter into the Exchange of Letters for the purpose of providing a framework for co-operation in the context of their respective tasks as well as mutual understanding, and exchanging information and technical assistance pertaining to the insurance sector on a reciprocal basis, to the extent permitted by the applicable laws, regulations, and requirements.

DEFINITIONS

For the purposes of these Letters, the terms set out below have the assigned meanings unless the context requires otherwise:

Authority means:

1. EIOPA is a European Supervisory Authority and an independent advisory body to the European Parliament, the Council of the European Union and the European Commission, established under Regulation (EU) No. 1094/20101 ("The Regulation").

EIOPA's core responsibilities are as follows:

- to support the stability of the financial system, transparency of markets and financial products as well as contribute to the protection of policyholders, pension scheme members and beneficiaries. EIOPA is commissioned to monitor and identify trends, potential risks and vulnerabilities stemming from the micro-prudential level, across borders and across sectors;

- to ensure the orderly functioning and integrity of financial markets in the European Union, as well as to pursue a constructive dialogue and effective cooperation with supervisory authorities outside the European Union; and

- to contribute as a competent authority to colleges of supervisors ("EEA Colleges"), which may include third country subsidiaries and branches or financial groups having their headquarters in third countries and their subsidiaries or branches in the European Union.

2. The FSA was originally established in 2000 and became an external organ of the Cabinet Office under the Act for Establishment of the Financial Services Agency (Establishment Act) in 2001 as a result of the reorganisation of central government ministries. Under the Establishment Act, the FSA has statutory responsibility for regulation and supervision of financial institutions, including insurance companies in Japan;

3. EIOPA and the FSA shall be collectively referred to herein as the "Authorities";

Jurisdiction means the country, state or other territory, as the case may be, in which EIOPA or the FSA has legal authority, power, and/or jurisdiction by laws, regulations, and requirements;

Laws, regulations, and requirements means any laws, regulations, and requirements of the European Union in force, including those applying to EIOPA and those of Japan;

Requested Authority means the Authority to whom a request is made pursuant to these Letters;

Requesting Authority means the Authority that makes a request pursuant to these Letters; and

Insurance Company means:

- an insurance undertaking, captive insurance undertaking, third country insurance undertaking, reinsurance undertaking, captive reinsurance undertaking or a third country reinsurance undertaking as defined in Article 13 of Directive 2009/138/EC ("Solvency II") for EU companies;

- an insurance company, an insurance holding company, subsidiary of an insurance company or an insurance holding company, a foreigninsurance company, or other legal entity, that conducts insurance business or other activities related to insurance business, as stipulated in the Insurance Business Act (Act No. 105 of 1995), including those defined in Article 2, Paragraphs 2, 7, 16, and 18.

OBJECTIVES

These Letters set forth the basis upon which EIOPA and the FSA propose to provide for regulatory and supervisory co-operation, including the development and implementation of risk-based solvency frameworks, conduct of business supervision, mutual assistance, and the exchange of information.

The purpose of these Letters is to provide a framework for co-operation, increased mutual understanding, exchange of information, and technical assistance to the extent permitted by laws, regulations, and requirements which EIOPA and the FSA are subject to.

The Authorities confirm that they will continue to engage in dialogue to seek to identify areas for cooperation and may share information on regulatory developments of mutual interest, including the development of international standards.

The Authorities intend to use their best endeavours to ensure that the fullest mutual assistance is provided within the terms of these Letters and engage in consultations, as appropriate, on mutually agreeable approaches designed to enhance the integrity and the efficiency of their respective insurance markets, and the exercise of insurance market regulatory and supervisory functions within the framework.

These Letters do not modify or supersede any laws, regulations, and requirements in force in, or applying to, EIOPA, the FSA or the jurisdictions in which they are authorized to regulate or supervise the business of insurance and do not create any legally binding obligations on or confer any rights to, EIOPA or the FSA. These Letters are not intended to affect any arrangements in existence to which either of the Authorities is a participant.

To read more:
https://www.eiopa.europa.eu/sites/default/files/publications/letters/25_2_2021_eiopa-jfsa.pdf

https://www.eiopa.europa.eu/sites/default/files/publications/letters/letter-fsa-to-eiopa.pdf

Number 8

The future of capital is green

Ravi Menon, Managing Director of the Monetary Authority of Singapore, at IMAS-Bloomberg Investment Conference.

MAS Monetary Authority of Singapore

Ms Susan Soh, Chairman of IMAS
Mr Steven Yankelson, Head of ASEAN, Bloomberg
Distinguished guests, ladies and gentlemen, good afternoon.

The future of capital is green. There are three powerful forces driving this:

- growing recognition of climate change as a global priority;
- advances in approaches to sustainable investing; and
- changing investor preferences.

First, climate change has become a risk that is too important for investors to ignore.

- The world needs to sharply reduce greenhouse gas emissions if we are to limit global warming to well below 2, and preferably 1.5 degree Celsius above pre-industrial levels as committed under the Paris Agreement …

- … specifically, reducing carbon emissions by half from 2010 levels by 2030, and reaching net zero around 2050.

- This implies a major transformation of economies and societies – affecting how we work and how we live.

- The transition to a low-carbon economy will impact every sector.

It is not just about renewables and electric vehicles. Greening will have to take place across all industries – steel, cement, mining, buildings, construction, maritime, agriculture, the list goes on.

To read more: https://www.bis.org/review/r210310b.pdf

Number 9

Who Can Find My Devices? Security and Privacy of Apple's Crowd-Sourced Bluetooth Location Tracking System

Alexander Heinrich, Milan Stute, Tim Kornhuber, and Matthias Hollick

Cornell University

Abstract

Overnight, Apple has turned its hundreds-of-million-device ecosystem into the world's largest crowdsourced location tracking network called offline finding (OF).

OF leverages online finder devices to detect the presence of missing offline devices using Bluetooth and report an approximate location back to the owner via the Internet.

While OF is not the first system of its kind, it is the first to commit to strong privacy goals.

In particular, OF aims to ensure finder anonymity, untrackability of owner devices, and confidentiality of location reports.

This paper presents the first comprehensive security and privacy analysis of OF. To this end, we recover the specifications of the closed-source OF protocols by means of reverse engineering.

We experimentally show that unauthorized access to the location reports allows for accurate device tracking and retrieving a user's top locations with an error in the order of 10 meters in urban areas.

While we find that OF's design achieves its privacy goals, we discover two distinct design and implementation flaws that can lead to a location correlation attack and unauthorized access to the location history of the past seven days, which could deanonymize users.

Apple has partially addressed the issues following our responsible disclosure. Finally, we make our research artifacts publicly available.

Number 10

Cyber-attack on the European Banking Authority

The European Banking Authority (EBA) has been the subject of a cyber-attack against its Microsoft Exchange Servers, which is affecting many organisations worldwide. The Agency has swiftly launched a full investigation, in close cooperation with its ICT provider, a team of forensic experts and other relevant entities.

As the vulnerability is related to the EBA's email servers, access to personal data through emails held on that servers may have been obtained by the attacker. The EBA is working to identify what, if any, data was accessed. Where appropriate, the EBA will provide information on measures that data subjects might take to mitigate possible adverse effects.

As a precautionary measure, the EBA has decided to take its email systems offline. Further information will be made available in due course.

When email communication channels are restored, our Data Protection Officer, Jonathan Overett Somnier, can be contacted at dpo@eba.europa.eu. For any urgent query, please contact the press line on +33 1 86 52 7052

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.

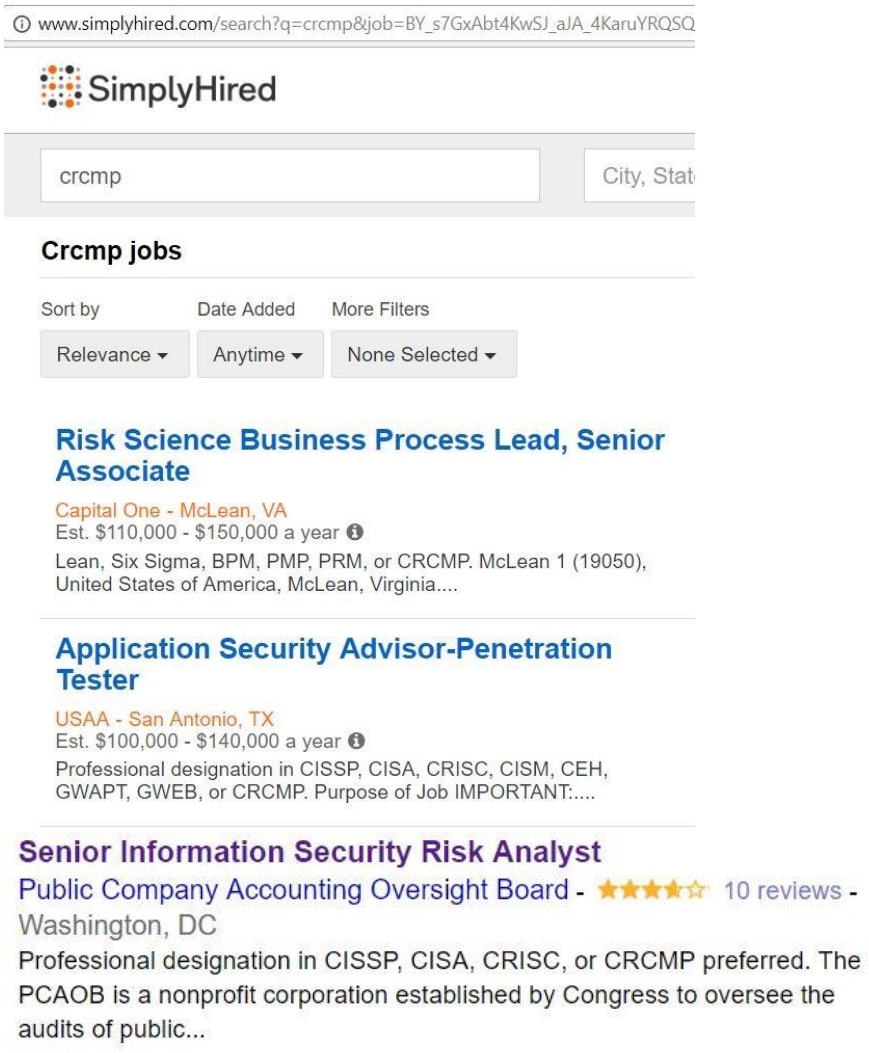
The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

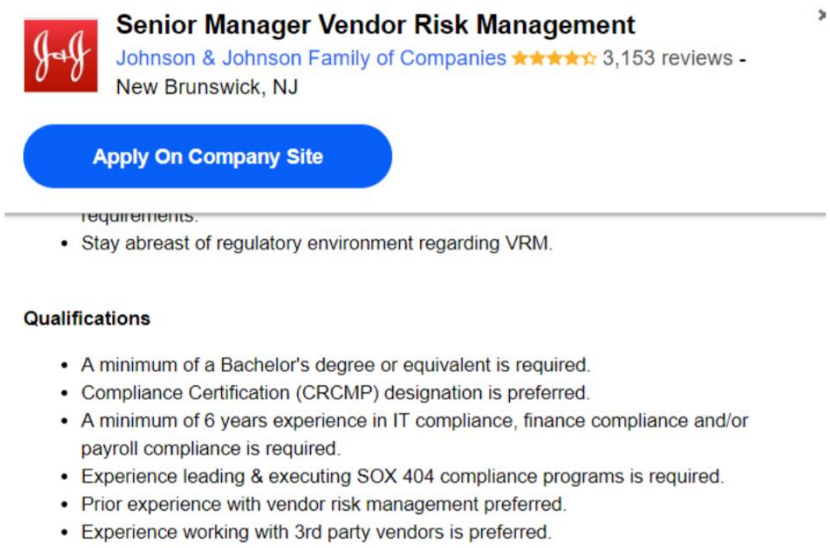
You can explore what we offer to our members:

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 around the world 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.