Monday, May 25, 2020

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,

This is scary.

1. Banks' performance on equity and debt markets since the Covid-19 outbreak has been on a par with that experienced after the collapse of Lehman Brothers in 2008.

2. During the initial phase, the market sell-off swept over all banks, which underperformed significantly relative to other sectors. Still, markets showed some differentiation by bank nationality, and credit default swap (CDS) spreads rose the most for those banks that had entered the crisis with the highest level of credit risk.

3. The subsequent stabilisation, brought about by forceful policy measures since mid-March, has favoured banks with higher profitability and healthier balance sheets. Less profitable banks saw their long-term rating outlooks revised to negative. And the CDS spreads of the riskiest banks continued increasing even through the stabilisation phase.

These are the key takeaways in an article at the *BIS Bulletin No 12 - Effects of Covid-19 on the banking sector: the market's assessment*.

We also read: The size and scope of the Covid-19 crisis, comparable so far to those of the Great Financial Crisis of 2007–09, imply that no banks will be left unscathed. The initial market reaction was a tsunami that engulfed many banks in a somewhat indiscriminate fashion.

A subsequent modest stabilisation revealed stronger differentiation, benefiting mainly better capitalised and more profitable banks, thus underscoring the value of healthy balance sheets. However, funding

conditions remain tight and long-term rating outlooks have been revised to negative for many banks, especially those with low profitability.

Meanwhile, actual ratings are starting to catch up with this trend, with more downgrades to be expected as the financial prospects of banks' borrowers deteriorate.

Despite a general price recovery in late April, markets remain wary of the longer-term prospects in the banking sector, especially its riskiest segments.

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

Best regards,

George Lekatis

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)

Internet Crime Complaint Center Marks 20 Years

From Early Frauds to Sophisticated Schemes, IC3 Has Tracked the Evolution of Online Crime

Number 2 (Page 11)

BIS Bulletin No 12 - Effects of Covid-19 on the banking sector: the market's assessment

Iñaki Aldasoro, Ingo Fender, Bryan Hardy and Nikola Tarashev

Number 3 (Page 12)

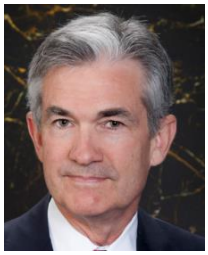
Presentation of the European Central Bank Annual Report 2019 to the Committee on Economic and Monetary Affairs of the European Parliament

Luis de Guindos, Vice-President of the European Central Bank, to the Committee on Economic and Monetary Affairs of the European Parliament, Frankfurt am Main.

Number 4 (Page 18)

Current economic issues

Jerome H Powell, Chair of the Board of Governors of the Federal Reserve System, Peterson Institute for International Economics, Washington DC.



Number 5 (Page 22)

Supervision and regulation report

Randal K Quarles, Vice Chairman for Supervision of the Board of Governors of the Federal Reserve System, before the Committee on Banking, Housing, and Urban Affairs, US Senate, Washington DC.

Number 6 (Page 24)

Manipulation ecosystem of social messaging platforms

Published by the NATO Strategic Communications Centre of Excellence

Number 7 (Page 26)

Publication of the list of Internationally Active Insurance Groups (IAIG) in the EU

eiopa
EUROPEAN INSURANCE AND OCCUPATIONAL PENSIONS AUTHORITY

Number 8 (Page 28)

Cybersecurity in the healthcare sector during COVID-19 pandemic

ENISA provides cybersecurity advice to support Hospitals and the healthcare sector against the increase of phishing campaigns and ransomware attacks during the coronavirus crisis.

enisa
European Network and Information Security Agency

Number 9 (Page 30)

The CCP-bank nexus in the time of Covid-19

BIS

Number 10 (Page 33)

Researchers on DARPA's Brandeis Program Enhance Privacy Protections for Android Applications

Privacy Enhancements for Android simplifies implementation of privacy protections for mobile apps running on Android OS

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Number 1

Internet Crime Complaint Center Marks 20 Years

From Early Frauds to Sophisticated Schemes, IC3 Has Tracked the Evolution of Online Crime

Throughout the 1990s, Americans took to the internet in droves. The decade saw the launch of the first web browsers, the introduction of now ubiquitous search engines, the birth of online commerce, and the ascendance of email as a go-to mode of communication.

As this new landscape bloomed, so did opportunities for criminals. The web offered easy access for cyber actors to target hundreds or even thousands of people at relatively low cost and risk.

When these crimes started occurring more frequently, the public was unsure where to turn for help. “People really didn’t know where to report internet scams or other online fraudulent activity,” said Internet Crime Complaint Center (IC3) Chief Donna Gregory. “And law enforcement agencies were saying: ‘What do we do with these? How do we handle them?’”

Recognizing the need to collect and assess information on cyber crime, the FBI started the Internet Fraud Complaint Center in May 2000 as a pilot project with the National White Collar Crime Center.

That center turns 20 this month. Renamed the Internet Crime Complaint Center (IC3) in 2002, the IC3 logged its 5 millionth complaint in March 2020. All that data has improved the public’s awareness of online crimes and helped the FBI and other law enforcement agencies better address internet-enabled attacks, fraud, thefts, and scams.

Online Crimes Grow More Damaging and Targeted

The crimes catalogued by the IC3 mirror the evolution of the web across two decades—growing in sophistication and number as the internet grows ever more essential to our professional and personal lives.

“The scale, scope, speed, and impact of cyber threats is constantly evolving,” said FBI Cyber Division Assistant Director Matt Gorham.

"Criminals are opportunistic, and we've seen them rapidly adapt to the cyber environment, creating a variety of schemes to exploit the public and private sector."

In its first full year of operation, the IC3 logged 49,711 complaints. Most of them revolved around internet auction fraud, non-delivery scams, and the West African letter (yes, that now infamous message from a prince or princess with an untapped fortune they wanted to share with you).

"People still fall victim to that letter and versions of it," said Gregory. "We still see scams that involve lotteries or windfalls where the victim just needs to pay what they believe are taxes or some fee to receive the winnings or a share of the fortune." Of course, there is no windfall to claim after the criminal collects those "fees" or "taxes."

"The scale, scope, speed, and impact of cyber threats is constantly evolving."
Matt Gorham, assistant director, FBI Cyber Division

"The more prevailing trend," said Gregory, who has been with the IC3 since its founding, "is that those early, rudimentary scams have given way to more destructive and costly data breaches and network intrusions, ransomware, romance scams, and sophisticated financial crimes like business email compromise."

Criminals still target individuals, but businesses and organizations are becoming more common targets because of the potential of a larger payout.

Losses recorded by the IC3 in recent years reflect the greater financial damage of this evolution. In 2019, victims reported more than $3.5 billion in losses—an average of $7,500 for each of the 467,361 complaints recorded that year. In 2001, the average victim lost $435.

Gregory said the IC3 has also seen a shift in the types of criminals perpetrating the illegal activity. Many of the criminals now live overseas, and organized crime groups are on the rise.

"The sophistication of modern online criminals is the most troubling part," Gregory said. "We used to be able to give people common sense tips to keep them safe; now it is just much harder to tell the real messages and websites from the fake."

Instead of an impersonal spam message with poor spelling and grammar, the scam may arrive via a well-written email that appears to come from a trusted colleague, business, or vendor.

Another enduring trend revealed in 20 years of crime data is that scammers will take advantage of a moment in time to prey on people who want to help or may need help in the wake of a natural disaster or tragic event.

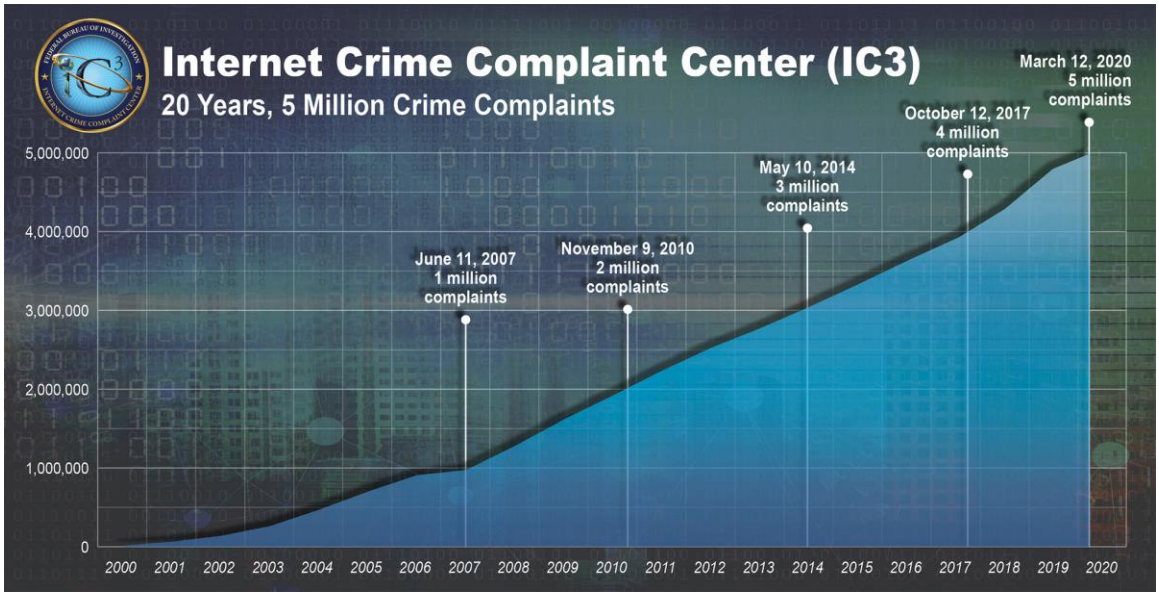
The center saw an uptick in charity and disaster fraud reports around the time of Hurricanes Rita and Katrina and after the Boston Marathon bombings.

In 2008, scammers tried to gather banking information from Americans waiting to receive stimulus checks as the nation slipped into recession.

Now, during the COVID 19 pandemic, scammers are working overtime hawking fake cures and investments schemes, selling protective equipment without the inventory on hand, and looking to take advantage of a more concentrated online presence during increased telework and distance learning arrangements.

“Criminals and scammers go where there is opportunity,” said Gorham. “Right now, they are exploiting a public health emergency to steal from and deceive people who are vulnerable, worried, or seeking vital supplies and assistance.”

“Those early, rudimentary scams have given way to more destructive and costly data breaches and network intrusions, ransomware, romance scams, and sophisticated financial crimes like business email compromise.” Donna Gregory, chief, IC3



Supporting Investigations

The IC3 collects and reports out its data in an annual report and educates the public by sending out notices about new scams or upticks in certain type of crimes. Its other key role is to support law enforcement. Federal, state, local, and tribal agencies can access the IC3's data through a secure database.

"The IC3 was created to provide the public and law enforcement with valuable information collected and analyzed by the FBI." Gorham stated. "By sharing this information, we hope to protect the American public from becoming victims of cyber crime and enable law enforcement to identify links and trends they may not otherwise be able to see."

Gregory also points to how IC3 data has helped improve the FBI's response to frauds carried out online. "We were seeing victims losing a lot of money, mostly through cases of business e-mail compromise," she said. "Initially we were able to work with financial institutions to examine wires going to international banks. Once we saw success in stopping some of those transactions, the criminals shifted to domestic accounts."

Gregory said money mules play a huge role in dividing up stolen money into U.S. accounts before moving it overseas. Money mules are people who allow criminals to use their bank accounts to launder illicit funds—either because they are receiving a commission for the service or because they trust the person asking for access to their account.

"Law enforcement could not keep up as the money started moving through U.S. accounts," Gregory said. "By the time they could take action, it was too late. So we started to look into working directly with the banks to stop the money flow and give law enforcement time to do the investigation."

In 2018, the FBI created the Recovery Asset Team to streamline communication with financial institutions and FBI field offices to halt fraudulent transactions faster. The team successfully recovered more than $300 million for victims in 2019.

After 20 years with the IC3, Gregory has learned that the online environment will continue to change and that the criminals will adapt along with it. She worries about the trends she's seeing in manipulated photos and videos but can never be certain where the next threat will emerge. The only things that are certain is that the IC3 will continue to evolve as well, finding new and better ways to warn and protect the public from cyber scams and support law enforcement as they combat the threat.

To report a crime or see the IC3's annual reports and warnings about current crimes, scams and frauds, visit ic3.gov.

For more information on common online crimes and prevention tips, visit the FBI's Common Scams and Crimes page.

To read more:
https://www.fbi.gov/news/stories/ic3-20th-anniversary-050820

Number 2

BIS Bulletin No 12 - Effects of Covid-19 on the banking sector: the market's assessment

Iñaki Aldasoro, Ingo Fender, Bryan Hardy and Nikola Tarashev

BIS

Banks have been harder hit than most sectors since the unsettlingly rapid global spread of Covid-19 sent financial markets into a tailspin.

This Bulletin examines markets' assessment of banks' performance thus far. The focus is on stock prices, credit default swap (CDS) and bond spreads, and credit ratings.

The price dynamics have been similar across equity and fixed income markets. Following generally contained declines during the early stages of the crisis, prices fell dramatically after 5 March, in a manner comparable to the immediate post-Lehman bankruptcy period.

A stabilisation and partial recovery set in shortly after the middle of the month, on the back of unprecedented policy measures taken by central banks and other authorities.

The policy measures also marked a turning point in terms of the extent to which investors were differentiating across banks according to their pre-pandemic characteristics.

During the initial period (from mid-February to mid-March), the sell-off was broad and quite indiscriminate, even though Chinese banks remained relatively unscathed and the riskiest banks experienced the largest increase in CDS spreads.

The differentiation became more pronounced during the stabilisation phase (from mid-March onwards), when profitability and balance sheet strength – as reflected in capitalisation, stable funding and credit ratings – became particularly good indicators of developments in bank stock prices, CDS spreads and rating outlooks.

The importance that markets attribute to strong balance sheets is likely to increase in an environment that sees a further weakening of borrowers' financial health.

To read more:
https://www.bis.org/publ/bisbull12.pdf

Number 3

Presentation of the European Central Bank Annual Report 2019 to the Committee on Economic and Monetary Affairs of the European Parliament

Luis de Guindos, Vice-President of the European Central Bank, to the Committee on Economic and Monetary Affairs of the European Parliament, Frankfurt am Main.

Madam Chair, Honourable Members of the Committee on Economic and Monetary Affairs, Ladies and gentlemen,

I welcome the opportunity to appear before this Committee today despite the difficult circumstances.

A strong relationship between the ECB and the European Parliament is more important than ever, as Europe is confronted with an extraordinary crisis. In addition to the health emergency, the coronavirus, or COVID-19, pandemic poses severe economic challenges to the euro area.

Through exchanges such as this we can demonstrate and explain how EU institutions are acting, within their mandate, to serve the European people in these difficult times.

Today we are publishing the ECB's Annual Report for 2019, together with the written feedback on your resolution on our previous Annual Report. Since the cut-off date for the Annual Report 2019, the outbreak of the COVID-19 pandemic has had significant effects on the economy and the ECB has taken extraordinary measures in response to this crisis.

Therefore, allow me to focus my remarks on the current economic environment. I am of course also happy to discuss the ECB's activities in 2019 as covered in the Annual Report, and answer any questions you may have about them.

I will start by presenting the assessment of the economic outlook and the measures taken by the ECB thus far. I will then discuss in more detail the impact of the COVID-19 pandemic on the financial sector, and conclude by

examining the role that the EU's financial agenda could play in the recovery phase.

The 2020 economic outlook and the ECB's recent decisions

Europe and the world are facing an economic contraction of extraordinary magnitude and speed. The measures imposed to contain the spread of the coronavirus have largely halted many economic activities. While these containment measures hit the services sector immediately, they also took their toll on the manufacturing sector.

According to preliminary estimates, the euro area economy contracted by 3.8 percent quarter on quarter in the first quarter of 2020, which only partially reflects the severity of the ensuing downturn. Consumer and business sentiment indicators for April have in fact plunged, suggesting an even larger contraction in the second quarter.

Labour market conditions have deteriorated dramatically, as indicated by the unprecedented take-up rate of employment support schemes. Of course, these government measures should help to support jobs and income and hence cushion consumption in these difficult circumstances.

Looking ahead, we are faced with a cloud of uncertainty about the course of the pandemic and the economic damage it will leave behind, which makes the job of forecasting macroeconomic developments more difficult than usual.

Growth scenarios prepared by ECB staff suggest that, this year, GDP could fall by between 5 percent in a mild scenario and 12 percent in a severe scenario. As the containment measures are gradually lifted, these scenarios foresee a recovery in economic activity.

Obviously, the extent of the contraction and the recovery will depend crucially on how long the containment measures are in place, the extent to which supply capacity and domestic demand are permanently affected, and the success of policies to mitigate the economic impact for businesses and workers.

As regards inflation developments, headline inflation decreased further, to 0.4 percent in April (from 0.7 percent in March) according to first estimates, mainly due to the large drop in oil prices. Based on current oil price expectations, inflation is likely to fall much further in the coming months.

In this unprecedented environment, the decisive and targeted policy measures the ECB has taken since early March have provided crucial support to the euro area economy, notably to those sectors most exposed to the crisis.

They support ample liquidity conditions, protect the smooth flow of credit to households and businesses, and preserve favourable financing conditions for all sectors and countries.

Under our pandemic emergency purchase programme, or PEPP, as well as under our other asset purchase programmes, by the end of this year we will have purchased more than €1 trillion of bonds.

These purchases, also thanks to their in-built flexibility, are helping to forestall an undue tightening of financing conditions and to counter the severe risks to the monetary policy transmission mechanism and the outlook for the euro area posed by the coronavirus pandemic.

We have made the conditions of our targeted longer-term refinancing operations (TLTRO III) substantially more attractive. We have also launched a new series of non-targeted pandemic emergency longer-term refinancing operations, or PELTROs, to ensure sufficient liquidity to the financial system.

Finally, we substantially eased our collateral rules to ensure that banks can make full use of our credit operations, ensuring that our monetary policy tools remain effective even in times of severe financial market stress and against the backdrop of looming rating downgrades.

Of course, as the economic situation is evolving rapidly, we are constantly monitoring the situation. We remain more determined than ever to ensure supportive financial conditions across all sectors and countries to allow this unprecedented shock to be absorbed.

We continue to stand ready to make further adjustments to our monetary policy measures should we see that the scale of the stimulus is falling short of what is needed.

The impact of the coronavirus emergency on the European financial sector

The pandemic hit the financial sector with an economic shock of unprecedented speed, scale and global scope. Unlike in 2008, the current crisis did not start in the financial system. But the spread of the virus

triggered a market reaction that at times rivalled the 2008 financial crisis in terms of the magnitude of price falls and volatility.

The tightening of market conditions was abrupt, broad-based and, at times, disorderly. Markets calmed following the announcement of forceful responses by monetary authorities around the globe. In particular, the ECB's announcement of private and public asset purchases has helped to restore market functioning in many asset classes.

In this challenging environment, banks' resilient balance sheets shielded them from the initial cash-flow shock. Recent efforts to build a stronger banking union allowed the banks to enter this crisis with healthier starting capital and liquidity positions than they had in 2008. At the end of 2019, the CET1 ratios of significant banks in the euro area stood at around 15 percent.

The creation of a solid institutional set-up enabled us to take swift action to ensure that the euro area financial system continues to play its role in mobilising savings and directing funds into the real economy. In addition to the monetary policy measures I already mentioned, the ECB also took a number of supervisory measures. I will not elaborate on them now because the Chair of the ECB's Supervisory Board discussed them before this Committee two days ago.

These measures will release some of the buffers that were built up during the good times and help banks to continue providing financial support to households and businesses hit by the economic fallout of the pandemic. Moreover, they will bring clear benefits in terms of maintaining a level playing field within the European banking sector.

These microprudential measures were complemented by a range of macroprudential actions. The ECB supports the swift action taken by national macroprudential authorities, which released or reduced capital buffer requirements.

In parallel, fiscal actions, the first line of defence at this point, provide essential support to the non-financial sector. These actions include tax breaks, public investment and generous fiscal backstops, such as public guarantees and credit lines.

While national support schemes are very welcome, the differences in their size and design could distort competition, as they have not been sufficiently coordinated at European level. Loan guarantees also strengthen the nexus between banks and non-financial corporations on the one side, and their sovereigns on the other.

As we move forwards, a European approach is important to ensure a level playing field and avoid fragmentation and the re-emergence of the bank-sovereign doom loop.

Overall, the euro area financial system has weathered much of the recent turmoil. But the loss of economic output and higher debt burdens increase the medium-term risk to financial stability in the euro area. Key vulnerabilities remain, in both the banking sector and the non-banking sector.

It will therefore be crucial to ensure that banks remain as robust as possible. The crisis should be seen as an opportunity to develop a vision for addressing pre-existing weaknesses in the banking sector and the crisis management framework for banks.

At the same time, the deteriorating profitability outlook for insurers, liquidity risk in investment funds and higher risk exposures of non-banks raise the risk of renewed strains on the financial system. These risks may warrant sector-specific policy action. Further reflections are also needed to develop an adequate macroprudential toolkit for this important and growing part of the financial system.

The road to recovery

Allow me to conclude with a few words on the road ahead, namely on the policy action that will be needed during the recovery.

ECB monetary policy will continue to provide the necessary support so that liquidity gets through to the people of Europe and the real economy. But our response will be made more powerful if all policies reinforce each other.

It is thus vital that the fiscal response to this crisis is sufficiently forceful, in all parts of the euro area. People and companies should be able to contribute to Europe's recovery wherever they are located. There now needs to be a political agreement to build the appropriate instruments for this common response, and I look forward to the upcoming discussions on the basis of the European Commission's proposal.

To propel the recovery forwards, Europe has a strong engine at its disposal: the Single Market, the EU's greatest achievement for its citizens.

As recognised by this Parliament just a few weeks ago, the Single Market is the source of our collective prosperity and well-being. So it is crucial that we repair, strengthen and deepen it in the coming months. And this is even truer for the financial sector. A genuinely integrated and resilient market is

essential to ensure financial stability and the financing of our economy. So progress on the capital markets union agenda is crucial.

Priority should be given to initiatives and proposals aimed at mobilising private savings and improving transparency and information for investors at the European level. Given the urgency of the situation, we should be open to any new and innovative ideas which can accelerate progress on the capital markets union.

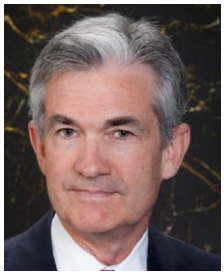
As Members of the European Parliament and the Committee on Economic and Monetary Affairs, you have an important role to play in bringing forward the legislative work on these dossiers.

Thank you, and I look forward to your questions.

Number 4

Current economic issues

Jerome H Powell, Chair of the Board of Governors of the Federal Reserve System, Peterson Institute for International Economics, Washington DC.



The coronavirus has left a devastating human and economic toll in its wake as it has spread around the globe. This is a worldwide public health crisis, and health-care workers have been the first responders, showing courage and determination and earning our lasting gratitude. So have the legions of other essential workers who put themselves at risk every day on our behalf.

As a nation, we have temporarily withdrawn from many kinds of economic and social activity to help slow the spread of the virus. Some sectors of the economy have been effectively closed since mid-March. People have put their lives and livelihoods on hold, making enormous sacrifices to protect not just their own health and that of their loved ones, but also their neighbors and the broader community. While we are all affected, the burden has fallen most heavily on those least able to bear it.

The scope and speed of this downturn are without modern precedent, significantly worse than any recession since World War II. We are seeing a severe decline in economic activity and in employment, and already the job gains of the past decade have been erased. Since the pandemic arrived in force just two months ago, more than 20 million people have lost their jobs.

A Fed survey being released tomorrow reflects findings similar to many others: Among people who were working in February, almost 40 percent of those in households making less than $40,000 a year had lost a job in March. This reversal of economic fortune has caused a level of pain that is hard to capture in words, as lives are upended amid great uncertainty about the future.

This downturn is different from those that came before it. Earlier in the post- World War II period, recessions were sometimes linked to a cycle of high inflation followed by Fed tightening. The lower inflation levels of recent decades have brought a series of long expansions, often accompanied by the buildup of imbalances over time-asset prices that reached unsupportable levels, for instance, or important sectors of the economy,

such as housing, that boomed unsustainably. The current downturn is unique in that it is attributable to the virus and the steps taken to limit its fallout. This time, high inflation was not a problem. There was no economy-threatening bubble to pop and no unsustainable boom to bust. The virus is the cause, not the usual suspects-something worth keeping in mind as we respond.

Today I will briefly discuss the measures taken so far to offset the economic effects of the virus, and the path ahead. Governments around the world have responded quickly with measures to support workers who have lost income and businesses that have either closed or seen a sharp drop in activity. The response here in the United States has been particularly swift and forceful.

To date, Congress has provided roughly $2.9 trillion in fiscal support for households, businesses, health-care providers, and state and local governments-about 14 percent of gross domestic product. While the coronavirus economic shock appears to be the largest on record, the fiscal response has also been the fastest and largest response for any postwar downturn.

At the Fed, we have also acted with unprecedented speed and force. After rapidly cutting the federal funds rate to close to zero, we took a wide array of additional measures to facilitate the flow of credit in the economy, which can be grouped into four areas.

First, outright purchases of Treasuries and agency mortgage-backed securities to restore functionality in these critical markets.

Second, liquidity and funding measures, including discount window measures, expanded swap lines with foreign central banks, and several facilities with Treasury backing to support smooth functioning in money markets.

Third, with additional backing from the Treasury, facilities to more directly support the flow of credit to households, businesses, and state and local governments.

And fourth, temporary regulatory adjustments to encourage and allow banks to expand their balance sheets to support their household and business customers.

The Fed takes actions such as these only in extraordinary circumstances, like those we face today. For example, our authority to extend credit directly to private nonfinancial businesses and state and local governments

exists only in "unusual and exigent circumstances" and with the consent of the Secretary of the Treasury. When this crisis is behind us, we will put these emergency tools away.

While the economic response has been both timely and appropriately large, it may not be the final chapter, given that the path ahead is both highly uncertain and subject to significant downside risks.

Economic forecasts are uncertain in the best of times, and today the virus raises a new set of questions: How quickly and sustainably will it be brought under control? Can new outbreaks be avoided as social-distancing measures lapse? How long will it take for confidence to return and normal spending to resume? And what will be the scope and timing of new therapies, testing, or a vaccine? The answers to these questions will go a long way toward setting the timing and pace of the economic recovery. Since the answers are currently unknowable, policies will need to be ready to address a range of possible outcomes.

The overall policy response to date has provided a measure of relief and stability, and will provide some support to the recovery when it comes. But the coronavirus crisis raises longer-term concerns as well.

The record shows that deeper and longer recessions can leave behind lasting damage to the productive capacity of the economy. Avoidable household and business insolvencies can weigh on growth for years to come. Long stretches of unemployment can damage or end workers' careers as their skills lose value and professional networks dry up, and leave families in greater debt.

The loss of thousands of small- and medium-sized businesses across the country would destroy the life's work and family legacy of many business and community leaders and limit the strength of the recovery when it comes. These businesses are a principal source of job creation-something we will sorely need as people seek to return to work.

A prolonged recession and weak recovery could also discourage business investment and expansion, further limiting the resurgence of jobs as well as the growth of capital stock and the pace of technological advancement. The result could be an extended period of low productivity growth and stagnant incomes.

We ought to do what we can to avoid these outcomes, and that may require additional policy measures. At the Fed, we will continue to use our tools to their fullest until the crisis has passed and the economic recovery is well under way. Recall that the Fed has lending powers, not spending powers.

A loan from a Fed facility can provide a bridge across temporary interruptions to liquidity, and those loans will help many borrowers get through the current crisis. But the recovery may take some time to gather momentum, and the passage of time can turn liquidity problems into solvency problems.

Additional fiscal support could be costly, but worth it if it helps avoid long-term economic damage and leaves us with a stronger recovery. This tradeoff is one for our elected representatives, who wield powers of taxation and spending.

Thank you. I look forward to our discussion.

Number 5

Supervision and regulation report

Randal K Quarles, Vice Chairman for Supervision of the Board of Governors of the Federal Reserve System, before the Committee on Banking, Housing, and Urban Affairs, US Senate, Washington DC.

Chairman Crapo, Ranking Member Brown, members of the Committee, thank you for the opportunity to testify today.

The past two months have been a time of exceptional economic hardship. The Congress has displayed an extraordinary willingness to act, in concert and at speed, to address this hardship and its wide-ranging consequences.

I appreciate your dedication to continuing our common work, as well as the chance to appear.

The report accompanying my testimony reviews supervisory and regulatory steps the Federal Reserve has taken to address the economic and financial challenges of the current economic contraction.

I do not plan to repeat those steps here, although I am happy to answer questions about them in detail. Instead, I will briefly outline the Federal Reserve's approach to supporting the nation's economy, maintaining the supply of credit, and reducing the economic impact of the various containment measures taken in response to public health concerns.

This approach applies, not only to our efforts thus far, but also to the efforts that we—and the financial sector—will make to support households and businesses in the months ahead.

It is worth a moment to acknowledge the profound effects of this crisis on the nation's financial system and economy.

The measures adopted to contain the pandemic triggered a deep, abrupt, and global financial shock. Uncertainty cascaded across the financial system.

Savers and investors, consumers and companies, took part in a flight to safety, seeking the stability of cash over the volatility of the markets.

No port was safe from the storm that followed, visiting asset classes from commercial paper to Treasury securities.

The strain it caused was widespread, as families and businesses struggled to pay their bills, meet their expenses, and sustain their daily lives.

More than a decade ago, U.S. banking organizations faced a different crisis, in which their structural weaknesses catalyzed and compounded the ongoing stress.

Twelve years of work—by Congress, financial institutions, and the regulatory agencies—went toward ensuring that this dynamic would not occur again.

Reforms, and other measures taken by the industry, raised the quantity and quality of bank capital, so banks could withstand a severe downturn and continue lending.

They established higher levels of liquidity, so banks could meet customer and counterparty demands.

They required improvements in risk management, so banks could avoid unexpected losses lurking in their books.

They improved operational resiliency, so banks could keep their doors open and their lights on after a shock. As a result, banks entered this crisis in a position of strength.

To read more:
https://www.bis.org/review/r200512a.pdf

Number 6

Manipulation ecosystem of social messaging platforms

Published by the NATO Strategic Communications Centre of Excellence

Social messaging platforms started as an alternative to the Short Messaging Service (SMS), pitching themselves as faster and cheaper, with additional features such as the ability to send documents and media securely.

These features granted users a level of encryption that meant no third party, including the messaging services themselves, was able to read the messages sent.

Today, social messaging platforms account for a combined 4.1 billion users and social messaging has become the most frequent activity a person carries out online.

Similarly to major social media platforms that are being artificially inflated and manipulated for financial and political gain, social messaging platforms are equally vulnerable to the threat of exploitation.

This study maps the online market for manipulation tools and services available for two popular messaging applications: WhatsApp and Telegram.

In doing so, we assess the effectiveness of these tools and services against the protective mechanisms put up by the messaging applications.

This publication aims to provide national institutions and communications practitioners with an overview of the scale and effect of manipulation on these popular social messaging platforms.

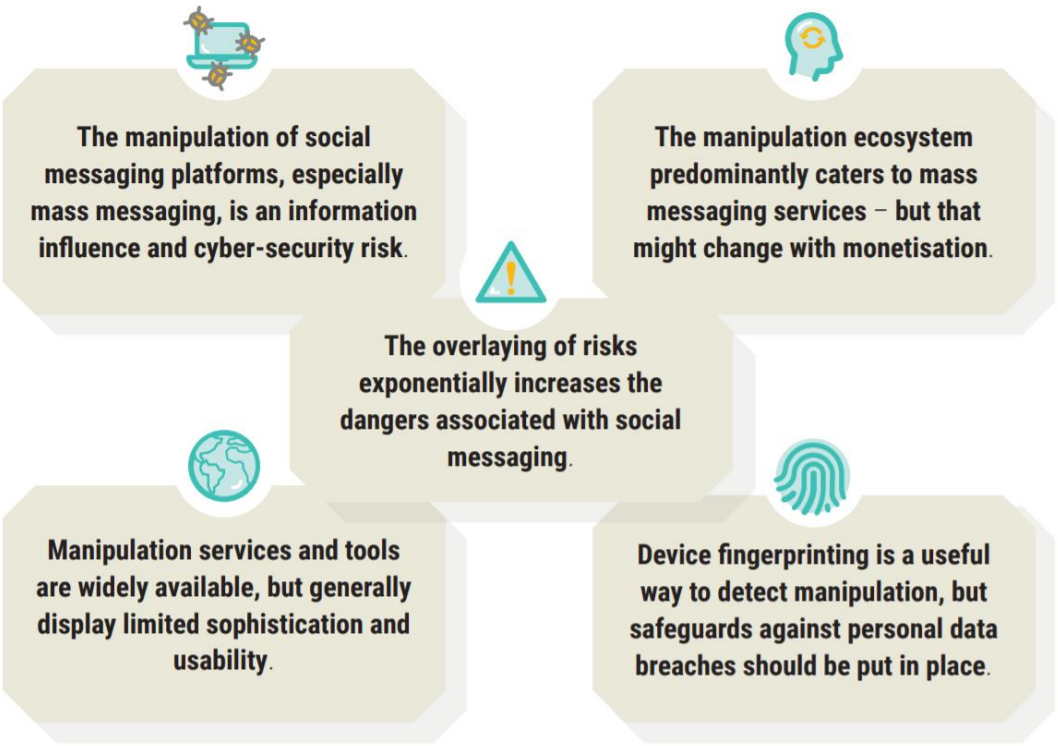
In collaboration with Singularex, a Ukrainian social media analytics company, we conducted the study in two parts.

The first part consisted of a landscape scan of the manipulation tools and services available for WhatsApp and Telegram.

We searched the web and spoke to sellers and freelancers over a period of two months to understand what a customer, or a potential malign actor, can purchase online. Given that previous research on social media had shown no significant difference between social media manipulation services

available on the dark web and the open web, we decided to focus our efforts on finding as diverse a group of services on the open web as we could.

The second part involved assessing the tools and services identified. This included evaluating the cost, methods and scale of manipulation available, the quality of manipulation tools and services, and the ability of WhatsApp and Telegram to identify and counter manipulation on their platforms.



To read more:
https://www.stratcomcoe.org/manipulation-ecosystem-social-messaging-platforms

Number 7

Publication of the list of Internationally Active Insurance Groups (IAIG) in the EU

The European Insurance and Occupational Pensions Authority (EIOPA) has published the list of Internationally Active Insurance Groups (IAIGs) headquartered in the EU.

IAIGs are the focus of the International Association of Insurance Supervisors (IAIS) Common Framework for the Supervision of Internationally Active Insurance Groups (ComFrame).

ComFrame identifies an IAIG as being an insurance group that meets two criteria, related to its international activity and size.

The list is based on information from those European group-wide supervisors that have shared with EIOPA their own list as of 12 May 2020, according to the criteria and cases set out in ComFrame (23.0.a and 23.0.b).

The insurance groups identified as of 12 May 2020 as Internationally Active Insurance Groups (IAIG) headquartered in the EU are:

- Aegon N.V.
- Ageas SA/NV
- Allianz SE
- Assicurazioni Generali S.p.A.
- Grupo Mapfre
- HDI Haftpflichtverband der Deutschen Industrie V.a.G.
- Münchener Rückversicherungs-Gesellschaft Aktiengesellschaft in München
- NN Group N.V.
- Vienna Insurance Group AG Wiener Versicherung Gruppe

Additional lists of European IAIGs are expected to be published soon.

The list is for informational purposes and should be used only in conjunction with ComFrame.

This list may be subject to change. For the up to date list of IAIGs please check List of Internationally Active Insurance Groups (IAIGs) headquartered in the EU at:
https://www.eiopa.europa.eu/tools-and-data/registers/list-internationally-active-insurance-groups-iaigs-headquartered-eu_en

Number 8

Cybersecurity in the healthcare sector during COVID-19 pandemic

ENISA provides cybersecurity advice to support Hospitals and the healthcare sector against the increase of phishing campaigns and ransomware attacks during the coronavirus crisis.

The COVID19 pandemic has created a new reality for the healthcare sector globally testing its limits.

Adding to the overwhelming situation it is currently facing, the sector has become a direct target or collateral victim of cybersecurity attacks.

Malicious actors taking advantage of the COVID19 pandemic have already launched a series of phishing campaigns and ransomware attacks.

Hospitals have shifted their focus and resources to their primary role, managing this extraordinary emergency, which has placed them in a vulnerable situation.

Hospitals, and the whole healthcare sector, now have to be prepared.

Cybercrime adapts to the world around it. It is hardly surprising that in the beginning of an escalating global pandemic like COVID-19, malware actors have jumped on the bandwagon.

The current situation in the EU and worldwide provides a fertile breeding ground for various campaigns. In no particular order, the following conditions are being exploited making the sector even more vulnerable:

- High demand for certain goods like protective masks, disinfectants and household products

- Decreased mobility and border closures

- Increasing reliance on teleworking, often with little previous experience and planning

- Increased fear, uncertainty and doubt in the general populatio

ENISA can provide some advice to support the sector, taking into account the situational evolution and most common incidents since the beginning of the pandemic.

- Share the information with healthcare staff in the organisation, build awareness of the ongoing situation and, in the case of infection, ask staff to disconnect from the network to contain the spread.

  Raise awareness internally in healthcare organisations and hospitals by launching campaigns even during the time of crisis (i.e. to inform hospital staff not to open suspicious emails).

- In case of systems compromise, freeze any activity in the system. Disconnect the infected machines from others and from any external drive or medical device. Go offline from the network. Immediately contact the national CSIRT.

- Ensure business continuity through effective backup and restore procedures. Business continuity plans should be established whenever the failure of a system may disrupt the hospital's core services and the role of the supplier is such cases must be well-defined.

- In case of impact to medical devices, incident response should be coordinated with the device manufacturer.

  Collaborate with vendors for incident response in case of medical devices or clinical information systems.

- One preparedness measure is network segmentation. With network segmentation network traffic can be isolated and / or filtered to limit and / or prevent access between network zones.

The whole cybersecurity community is working together to support the healthcare sector as the pandemic develops; national cybersecurity authorities are issuing alerts and guidelines (e.g. the situation in CZ) on potential cyber attacks; in the CSIRT Network MS continuously exchange information and issue situational reports together with the EU Institutions; the private sector is offering pro-bono cybersecurity related services supporting the healthcare sector.

For further information related to the cybersecurity aspects of the COVID19 pandemic, consult the ENISA pages dedicated to this issue under the Topic COVID19 at: https://www.enisa.europa.eu/topics/wfh-covid19

Number 9

The CCP-bank nexus in the time of Covid-19

BIS

Key takeaways

- During the Covid-19-induced financial turbulence, central counterparties (CCPs) issued large margin calls, weighing on the liquidity of clearing member banks.

- In spite of the turbulence, CCPs remained resilient, as intended by the post-crisis reforms of financial market infrastructures.

- Higher margins should be expected during heightened turbulence, but the extent of the procyclicality of margining is the consequence of various design choices.

- Systemic considerations call to examine the nexus between banks and CCPs. Therefore, when thinking about margining, central banks need to assess banks and CCPs jointly rather than in isolation.

The Covid-19 pandemic led to market turmoil in mid-March. Large price movements prompted large margin calls from central counterparties (CCPs).

This strained the liquidity positions of large dealer banks. Banks also hoarded liquid assets, possibly in anticipation of large margin calls.

This exacerbated the liquidity squeeze. Nevertheless, CCPs remained resilient, vindicating the post-crisis reforms that incentivised central clearing.

The procyclicality of leverage embedded in margining models might have played a role in the events of mid-March.

These margin models are critical because they underpin the management of counterparty credit risk.

Margin models of some CCPs seem to have underestimated market volatility, in part because they have relied on a short period of historical price movements from tranquil times.

These CCPs had to catch up and increase margins at the wrong time, squeezing liquidity when it was most needed.

Going forward, the interaction of CCPs with clearing member banks is critical ("CCP-bank nexus").

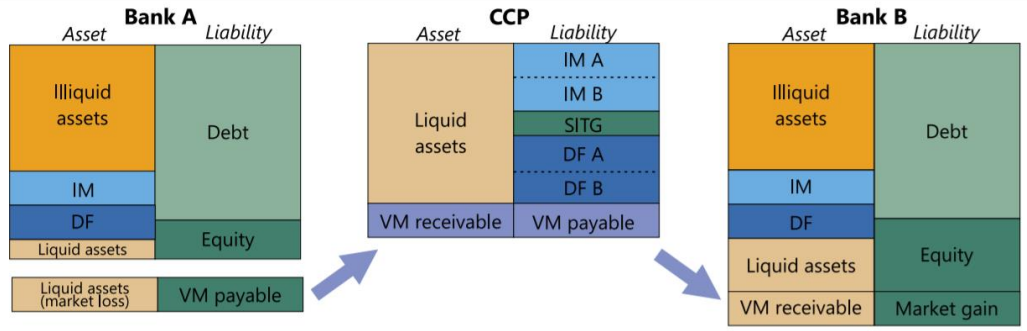
Importantly, actions that might seem prudent from an individual institution's perspective, such as increasing margins in a turmoil, might destabilise the nexus overall.

Therefore, central banks need to assess banks and CCPs jointly rather than in isolation.

Mechanism of CCP margining

A CCP stands between two clearing members and insures them against counterparty credit risk (Graph 1).

CCP and bank balance sheets as the price of a cleared contract changes — Graph 1



DF = default fund; IM = initial margin; SITG = CCP skin in the game; VM = variation margin.

Source: Faruqui, Huang and Takáts (2018).

The CCP uses two kinds of margin to manage counterparty credit risk: variation margin (VM) and initial margin (IM).

VM transfers marked-to-market profits and losses: when prices move, members with losing positions pay VM to the CCP and the CCP pays VM to members with winning positions (purple boxes).

After VM payments, positions have zero value again. In contrast, IM is collected to cover potential changes in the value of a member's portfolio over some future period (light blue boxes).

Margining transforms counterparty credit risk into liquidity risk: VM payments settle current market exposure and IM covers potential future exposure – but liquidity risk remains due to these margin calls. Furthermore, the effects of IM and VM calls on liquid assets are different. VM calls transfer liquid assets from the losing party to the winning one – thereby having a distributional effect.

In contrast, IM calls absorb liquid assets from all banks onto the CCP balance sheet – thereby having an aggregate effect.

To read more:
https://www.bis.org/publ/bisbull13.pdf

Number 10

Researchers on DARPA's Brandeis Program Enhance Privacy Protections for Android Applications

Privacy Enhancements for Android simplifies implementation of privacy protections for mobile apps running on Android OS

From navigation to remote banking, mobile device users rely on a variety of applications to streamline daily tasks, communicate, and dramatically increase productivity.

While exceedingly useful, the ecosystem of third-party applications utilizes a number of sensors – microphones, GPS, pedometers, cameras – and user interactions to collect data used to enable functionality.

Troves of sensitive personal data about users are accessible to these applications and as defense and commercial mobile device users become increasingly reliant on the technology, there are growing concerns around the challenge this creates for preserving user privacy.

Under DARPA's Brandeis program, a team of researchers led by Two Six Labs and Raytheon BBN Technologies have developed a platform called Privacy Enhancements for Android (PE for Android) to explore more expressive concepts in regulating access to private information on mobile devices.

PE for Android seeks to create an extensible privacy system that abstracts away the details of various privacy-preserving technologies, allowing application developers to utilize state-of-the-art privacy techniques, such as secure multi-party computation and differential privacy, without knowledge of their underlying esoteric technologies.

Importantly, PE for Android allows mobile device users to take ownership of their private information by presenting them with more intuitive controls and permission enforcement options.

The researchers behind PE for Android today released a white paper detailing the platform's capabilities and functionality, and published an open source release of its code to GitHub.

In open sourcing PE for Android, the researchers aim to make it easier for the open-source Android community and researchers to employ enhanced privacy-preserving technologies within Android apps while also

encouraging them to help address the platform's current limitations and build upon its initial efforts.

"User privacy should be a first-rate concern for mobile app development, and we are hoping that open-sourcing PE for Android will galvanize the Android developer community," said Dr. Josh Baron, the DARPA program manager leading Brandeis.

"While the benefits of this to personal and commercial users may be apparent, military personnel are also heavy users of mobile devices and often bring personal devices to or near work. Changes made to the Android ecosystem will therefore have important implications for privacy and security across the Department of Defense. I encourage the community to take a look at the code, improve it if they find gaps, and figure out which parts are deserving of adoption into the broader Android ecosystem."

PE for Android is comprised of a set of extensions and interfaces that are integrated into the Android OS. The primary components, which include APIs, services, and a Privacy Abstraction Layer (PAL), are invoked when applications request private data.

Apps employing PE for Android can opt to send these requests to the platform's Private Data Service and associated modules called µPALs, where data transformation and isolation techniques are implemented to convert private data into less sensitive forms.

This moves sensitive data processing out of the application process space where there is a higher risk of intentional or unintentional data leakage, and into secure services that implement privacy-preserving technologies.

Once the sensitive information is transformed, it may then be returned to the application. Under this model, only the trusted architecture of the Private Data Service – not the requesting app – has direct access to the full scope of sensitive data available through the stock Android API.

Another key component of PE for Android are Policy Managers. This API helps provide fine-grained control of permissions; enabling users to more easily specify their privacy policy and gain greater control over how their private information is used.

Through Policy Managers, users are provided additional context around why the information is needed and how it will be used within a given application. From there, they can make a more informed decision as to what information the application will be given access too.

The PE for Android source code release includes several use cases and applications for these key components, many of which were developed by other research teams working under the Brandeis program.

This includes a Privacy Checkup tool; the Purposes Policy Manager developed by Carnegie Mellon University, which lets people view and set policies for individual apps as well as all apps on a smartphone; and various μPAL modules capable of performing privacy transformations on different types of sensitive data.

The University of Vermont and the Brandeis Helio team are among those responsible for developing the μPAL modules discussed in the white paper.

Additional information about PE for Android is available at:
https://android-privacy.org

Disclaimer

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

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

This information:

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

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

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

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

- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);

- is in no way constitutive of an interpretative document;

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

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

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts.

It is our goal to minimize disruption caused by technical errors.

However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

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

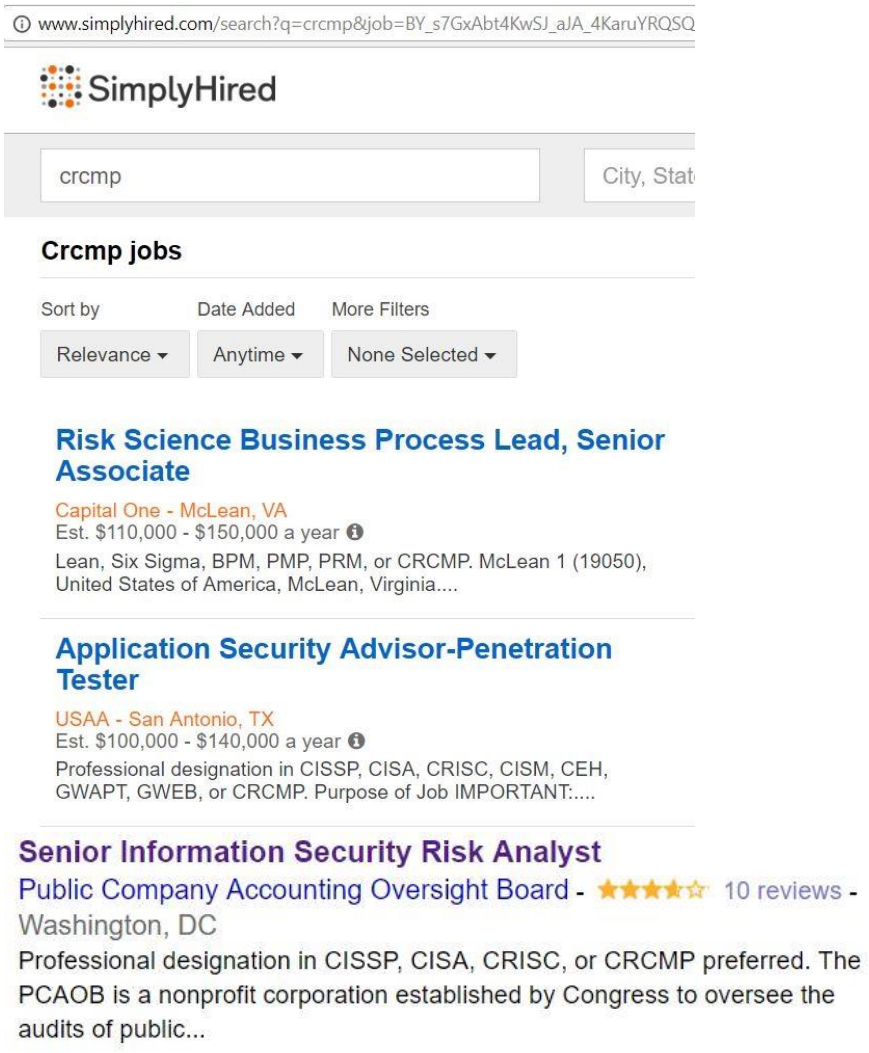
International Association of Risk and Compliance Professionals

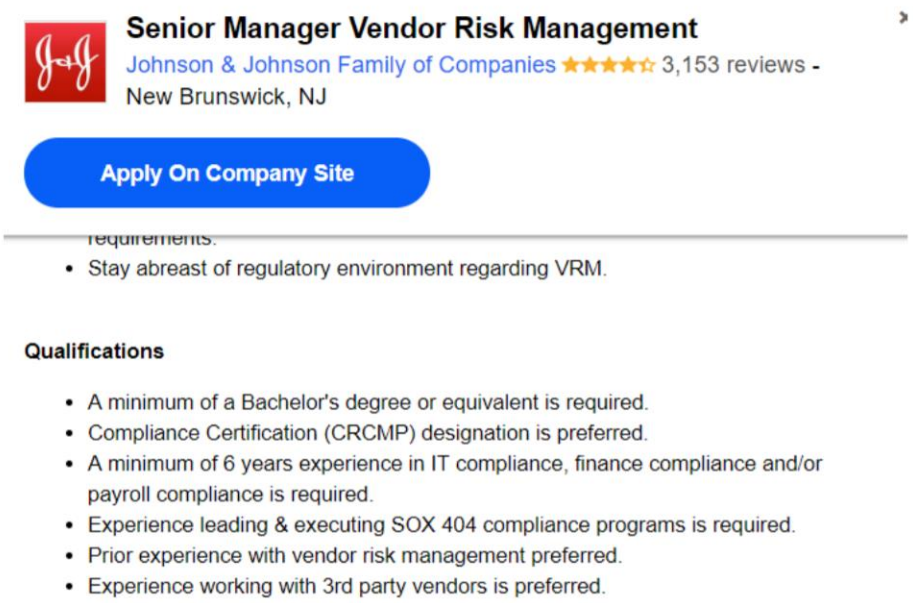
You can explore what we offer to our members:

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.

4. *IARCP Authorized Certified Trainer (IARCP-ACT) Program* - This is an additional advantage on your resume, serving as a third-party endorsement to your knowledge and experience.

Certificates are important when being considered for a promotion or other career opportunities. You give the necessary assurance that you have the knowledge and skills to accept more responsibility.

To learn more, you may visit:
https://www.risk-compliance-association.com/IARCP_ACT.html

5. *Approved Training and Certification Centers (IARCP-ATCCs)* - In response to the increasing demand for CRCMP training, the International Association of Risk and Compliance Professionals is developing a world-wide network of Approved Training and Certification Centers (IARCP-ATCCs).

This will give the opportunity to risk and compliance managers, officers, and consultants to have access to instructor led training at convenient locations that meet international standards.

ATCCs use IARCP approved course materials and have access to IARCP Authorized Certified Trainers (IARCP-ACTs).

To learn more:
https://www.risk-compliance-association.com/Approved_Centers.html