*Monday, January 18, 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,

The UK left the EU on 31 January 2020 with a Withdrawal Agreement, and entered a transition period that ended on 31 December 2020. On 24 December 2020, the UK and the EU agreed on the terms of the UK-EU Trade and Cooperation Agreement. The UK has approved the agreement and it came into effect provisionally on 31 December 2020, pending the EU taking the necessary steps to fully approve it.

The main problem for risk and compliance professionals is that *passporting between the UK and the EEA has ended.* For years, passporting had allowed firms authorised in European Economic Area (EEA) states to conduct business in *other* EEA states based on their 'home' member state authorisation. However, passporting between the UK and EEA states ended with the close of the transition period at 11pm on 31 December 2020.

This affects firms and funds based in the:

- UK that conduct certain types of business in the EEA,
- EEA that carry out certain types of business in the UK.

If your firm *transfers personal data* between the UK and the EEA, you should be aware of the new data rules that are now in place.

The UK Government has legislated so that UK firms can continue to lawfully send personal data from the UK to the EEA and 13 other countries that the EU has deemed to provide an adequate level of protection of personal data.

The UK Government has also announced that the UK-EU Trade and Cooperation Agreement provides for the continued free flow of personal data from the EU and EEA to the UK until adequacy decisions are adopted, for no longer than 6 months.

The UK's Information Commissioner's Office (ICO) is the regulator for data protection issues in the UK. Read the ICO's information on data protection and Brexit.

The ICO has said that the agreement between the UK and the EU enables businesses and public bodies across all sectors to continue to freely receive data from the EU (and EEA). However, as a sensible precaution, the ICO recommends that businesses work with EU and EEA organisations who transfer personal data to them, to put in place alternative transfer mechanisms to safeguard against any interruption to the free flow of EU to UK personal data.

You should also consider taking legal advice if you believe that you might be affected. *Read more at number 2 below*.

Another important development: The COVID-19 pandemic has given rise to a defining change for community banks: a *broader use of technology,* both at present and for the future.

The pandemic has resulted in branch closures, stay-at-home orders, and a general desire to limit direct contact, all of which has increased the use of computers, mobile phones, and other smart devices to complete financial services transactions.

To meet growing demand, community banks have used both direct investment and contracts with technology service providers and fintechs to accelerate their adoption of technologies that enable such services as remote deposit, online applications, peer-to-peer payments, and electronic signatures.

We can find the above information at the *Community Banking Study, December 2020,* from the Federal Deposit Insurance Corporation (FDIC). This is a great paper (129 pages). We read:

"Some community banks, for example, used technology to help manage the unprecedented volume of loan applications received in response to the Small Business Administration's (SBA) *Paycheck Protection Program (PPP).* Over the span of a few months, community banks provided billions of dollars of needed credit to small and medium-sized enterprises through

the program, with 3,843 community banks holding over $148 billion in PPP loans as of June 30, 2020.

Arguably, technology facilitated this lending by allowing some community banks to accept applications and supporting documentation online, process applications faster, and submit files for SBA approval.

As the PPP moves into its next phase, community banks are also seeking the aid of technology to automate loan forgiveness applications. Not all accounts from community bankers and borrowers about using technology to assist with PPP lending were positive, however, nor is it clear that technology increased the use or efficiency of the program.

Reports of difficulties connecting with SBA's systems (E-Tran) and last-minute changes to the program, including a ban on robotic data entry systems, suggested a limit to the effectiveness of technology.

Nonetheless, at least among community banks in the 2019 CSBS survey, those identified in this chapter as high-technology adopters showed greater participation in the program, with PPP loans totalling 6.5 percent of assets, compared with 5.7 percent of assets for medium-adopting banks and 5.0 percent of assets for low-adopting banks.

Future research may better identify the extent to which technology facilitated PPP lending as well as other credit during the pandemic.

The degree to which banks continue after the pandemic to rely on technology investments and partnerships made during the pandemic remains unknown; however, it seems unlikely that customers' use of technology will return to pre-pandemic levels even after branches and the economy resume normal operations.

In a PriceWaterhouseCoopers (PwC) survey of 6,000 U.S. bank customers conducted in May and June 2020, 24 percent stated they were less likely to use their bank's branch offices.

In addition, following months of remote work, banks (like many other businesses) may consider permanent changes to workspaces, which could have long-term effects on branch structure and operating expenses.

It is also possible that because of the pandemic, technology adoption by community banks will decrease. Banks that experience financial hardship may have reduced ability and desire to invest in new technology, a development suggested by the findings of this chapter associating revenues and local economic growth with technology adoption.

And post-pandemic, some community banks may experience less of a decline to branch traffic, a development suggested by the number of respondents to the PwC survey who indicated they were likely to continue using branch offices, including for services that can be done remotely."

Heraclitus believed that *there is nothing permanent except change*. Winston Churchill has said *to improve is to change; to be perfect is to change often*. COVID-19 is a major challenge, it can also become an opportunity.

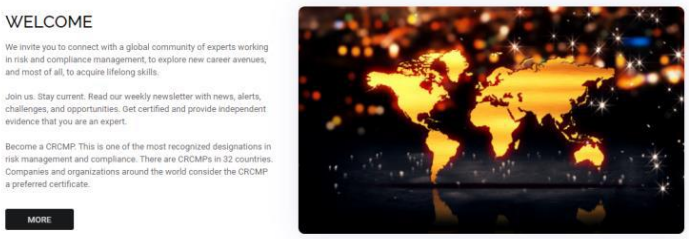
Read more at number 1 below. Welcome to the top 10 list.

*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

*Visit our updated website: https://www.risk-compliance-association.com*

INTERPOL

*Number 7 (Page 29)*

## The Cybersecurity Strategy

European Commission

*Number 8 (Page 32)*

## Response to COVID-19 and medium- to long-term challenges for Japan's economy - with an eye on the post-COVID-19 era

Haruhiko Kuroda, Governor of the Bank of Japan, at the meeting of Councillors of Nippon Keidanren (Japan Business Federation), Tokyo.

*Number 9 (Page 37)*

## Microsoft Internal Solorigate Investigation Update

Microsoft

*Number 10 (Page 39)*

## SolarWinds filing with the Securities and Exchange Commission

**CURRENT REPORT**

**PURSUANT TO SECTION 13 OR 15(d) OF**
**THE SECURITIES EXCHANGE ACT OF 1934**

**December 14, 2020**
**Date of Report (Date of earliest event reported)**

---

**SOLARWINDS CORPORATION**
**(Exact name of registrant as specified in its charter)**

*Number 1*

## FDIC Community Banking Study, December 2020

Eight years ago, coming out of the financial crisis, the FDIC conducted a study of community banks. This study was the first large-scale review of community banks ever conducted, and it recognized the importance of community banks and their unique role in the banking industry.

As a result of that study, the FDIC changed its approach to identifying community banks. In general, community banks are those that provide traditional banking services in their local communities.

As of year-end 2019, there were 4,750 community banks in the country with more than 29,000 branches in communities from coast to coast.

Since the 2012 study, community banks have proven to be resilient. Relative to noncommunity banks, community banks have had faster growth in return on assets ratios, higher net interest margins, stronger asset quality, and higher loan growth rates.

Community banks have continued to demonstrate this strength during the COVID-19 pandemic. The FDIC recognizes the role community banks play in providing loan and deposit services to customers throughout this country, which is why I made this update to the 2012 Community Banking Study a research priority in 2020.

I instructed my research team not only to update key aspects of the prior study, but also to consider new topics that are important to community banks, such as regulatory change and technology.

By continuing to study community banks and providing that research to the public—our stakeholders—we can continue to identify ways that the FDIC can provide support to these institutions. I would like to extend a special thanks to Diane Ellis, Director of the FDIC Division of Insurance and Research, for leading this effort.

I believe this work will provide continued recognition of community banks' strength, their unique role in the banking industry, and their value to the public.

*Jelena McWilliams Chairman, FDIC December 2020*

**Chart 1.1**

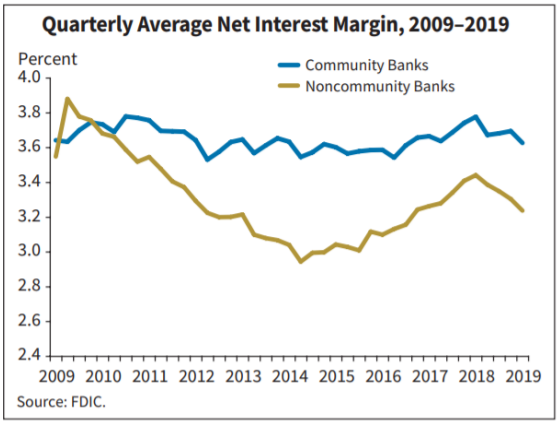



**Chart 1.2**

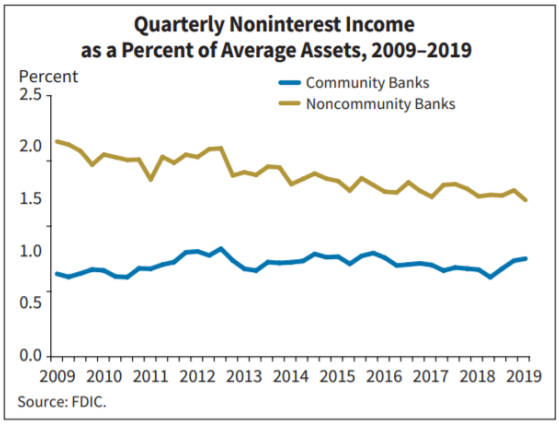



**Table 1.2 Assets With Maturities Greater Than 3 Years to Total Assets (Percent)**

| | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 |
|---|---|---|---|---|---|---|---|---|
| **All Banks** | **28.8** | **29.5** | **30.2** | **31.6** | **32.4** | **32.6** | **32.4** | **33.3** |
| Community Banks | 42.9 | 47.3 | 47.9 | 47.4 | 47.2 | 46.8 | 45.8 | 44.8 |
| Noncommunity Banks | 26.5 | 26.7 | 27.5 | 29.2 | 30.2 | 30.5 | 30.4 | 31.8 |

Source: FDIC.

**Table 1.3 Noninterest Income at Community and Noncommunity Banks (Percent)**

| Category of Noninterest Income as a Percent of Total Noninterest Income | Full-Year 2012 | | Full-Year 2019 | |
|---|---|---|---|---|
| | Community Banks | Noncommunity Banks | Community Banks | Noncommunity Banks |
| Service Charges on Deposit Accounts | 24.3 | 12.7 | 18.8 | 13.1 |
| Fiduciary Income | 6.9 | 11.9 | 8.0 | 14.3 |
| Gains on Asset Sales | 21.7 | 3.9 | 22.0 | 4.0 |
| Market Sensitive Income[1] | 2.6 | 11.8 | 3.0 | 17.6 |
| Securitization Income | 0.5 | 0.6 | 0.1 | 0.1 |
| Servicing Income | 3.1 | 4.7 | 3.7 | 1.2 |
| Insurance Income | 3.3 | 1.4 | 3.1 | 1.7 |
| All Other Noninterest Income[2] | 37.5 | 53.0 | 41.4 | 47.9 |
| **Total Noninterest Income** | **100.0** | **100.0** | **100.0** | **100.0** |
| Noninterest Income as a Percent of Net Operating Revenue | 22.0 | 39.4 | 20.2 | 34.2 |
| Noninterest Income as a Percent of Average Assets | 0.95 | 1.9 | 0.87 | 1.5 |

Source: FDIC.

[1] Includes trading, venture capital, and investment banking income.

[2] Other noninterest income includes service charges, commissions, and fees (such as safe deposit box rentals, money orders and cashiers checks, notarizing of documents, ATM fees, wire transfers), check sales, rental income from other real estate owned, bank-owned life insurance income, annual credit card fees and interchange fees.

**Chart 1.3**

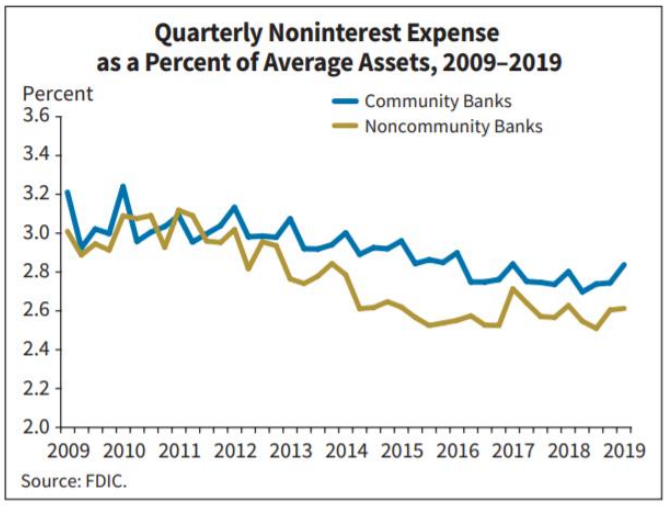


**Table 1.4 Compound Annual Growth Rate of Noninterest Expense Categories (Percent)**

| | Full-Year 2012 | | Full-Year 2019 | |
|---|---|---|---|---|
| | Community Banks | Noncommunity Banks | Community Banks | Noncommunity Banks |
| Salary and Employee Benefit Expenses | 4.6 | 7.0 | 1.4 | 3.0 |
| Premises and Fixed Asset Expenses | 3.2 | 5.2 | -0.8 | 0.7 |
| **Salary + Fixed Asset Expenses** | **4.3** | **6.6** | **1.0** | **2.6** |
| All Other Noninterest Expenses | 2.4 | 4.7 | -1.6 | 0.8 |
| **Total Noninterest Expenses** | **3.8** | **7.4** | **0.1** | **1.9** |
| **Average Assets** | **4.0** | **9.3** | **1.5** | **4.0** |

Source: FDIC.



To read the paper (129 pages):
https://www.fdic.gov/resources/community-banking/report/2020/2020-cbi-study-full.pdf

*Number 2*

## FCA, UK - Considerations for firms after the transition period

Following Brexit and the end of the transition period, find out about the temporary transitional power (TTP), considerations for UK and EEA firms, and how the end of passporting may affect you.

The UK left the EU on 31 January 2020 with a Withdrawal Agreement and entered a transition period that ended on 31 December 2020. On 24 December 2020, the UK and the EU agreed on the terms of the UK-EU Trade and Cooperation Agreement. The UK has approved the agreement and it came into effect provisionally at 11pm on 31 December 2020, pending the EU taking the necessary steps to fully approve it.

How this affects you will depend on several factors, including the nature of your business and where your customers are located. You should make sure you have considered the following points and understand the impact they could have on your firm:

## Considerations for all firms

*End of passporting*

Passporting between the UK and the EEA has now ended.

Passporting allows firms authorised in EEA states to conduct business in other EEA states based on their 'home' member state authorisation.

However, passporting between the UK and EEA states ended with the close of the transition period at 11pm on 31 December 2020.

This affects firms and funds based in the:

- UK that conduct certain types of business in the EEA

- EEA that carry out certain types of business in the UK

If you intend to do business in the EEA, you should ensure you do so consistent with local laws and local regulatory expectations, eg seeking authorisation with a local authority where appropriate.

*Converting EU legislation*

The European Union (Withdrawal) Act 2018 converted into UK law existing EU legislation that had direct effect in the UK at the end of the transition period. This also preserved existing UK laws that implemented EU obligations.

The Government was given powers to amend the retained EU legislation so it works in the UK after Brexit. It has used this power to make numerous statutory instruments that amend retained EU financial services legislation.

The Government's intention was that the same rules and laws continue to apply, as far as possible, but with the necessary amendments to reflect the UK's position outside the EU.

The Government gave us (and, where relevant, the Bank of England and the Prudential Regulation Authority) responsibility for amending and maintaining certain EU binding technical standards that have become UK law. These technical standards specify detailed requirements for the purposes of various EU regulations and directives.

We have amended our Handbook to make sure it's consistent with changes the Government has made, and so it still works effectively now that the transition period has ended.

For more information, read our statement on changes to UK legislation.

*Temporary transitional power (TTP)*

To help you adapt to your new requirements, the Treasury has given UK financial regulators the power to make temporary transitional provisions in relation to financial services legislation. This is known as the temporary transitional power (TTP).

We are applying the TTP on a broad basis from the end of the transition period until 31 March 2022. This means firms and other regulated persons can continue to comply with existing requirements for a limited period.

However, there are some areas where the TTP doesn't apply and where you are now expected to be compliant.

*Users of credit ratings*

We are now the UK regulator of UK-registered and certified credit rating agencies (CRAs).

This means that any UK legal entity that wishes to issue credit ratings publicly or by subscription will need to be registered or certified with us as a CRA. These CRAs have made system changes to flag ratings that are available for regulatory use in the UK.

If you use credit ratings for regulatory purposes, you should use credit ratings issued or endorsed by FCA-registered CRAs. You should have contacted the relevant CRAs whose ratings you use, to understand the systems changes they've made.

*Data sharing*

If your firm transfers personal data between the UK and the EEA, you should be aware of the new data rules that are now in place.

The Government has legislated so that UK firms can continue to lawfully send personal data from the UK to the EEA and 13 other countries that the EU has deemed to provide an adequate level of protection of personal data.

The Government has also announced that the UK-EU Trade and Cooperation Agreement provides for the continued free flow of personal data from the EU and EEA to the UK until adequacy decisions are adopted, for no longer than 6 months.

The Information Commissioner's Office (ICO) is the regulator for data protection issues in the UK. Read the ICO's information on data protection and Brexit.

The ICO has said that the agreement between the UK and the EU enables businesses and public bodies across all sectors to continue to freely receive data from the EU (and EEA).

However, as a sensible precaution, the ICO recommends that businesses work with EU and EEA organisations who transfer personal data to them, to put in place alternative transfer mechanisms to safeguard against any interruption to the free flow of EU to UK personal data.

You should also consider taking legal advice if you believe that you might be affected.

*Communicating with customers*

You must pay attention to what your customers need to know, and communicate with them in a way which is clear, fair and not misleading (Principle 7).

We expect you to have contacted any of your customers who have been affected by the end of the transition period. We have made this clear in information we have published for consumers on how Brexit might affect them.

You should be able to show you have considered and planned for how the end of the transition period may have affected your customers. You should keep in mind that different categories of customers may have been affected in different ways, as is set out in our guidance in PRIN 1.2. You may visit: https://www.handbook.fca.org.uk/handbook/PRIN/2/1.html

For example, customers based in the EEA (including UK expats) may be more affected than those living in the UK. You should have contacted each group of customers, to explain clearly how they have been or will be affected.

As well as offering information directly to your customers, you should have made the important information available more widely, such as on your website. This also includes being prepared for the possibility that you may have a significant increase in consumer queries now that the transition period has ended.

We expect you to have communicated to your customers in good time – usually, the earlier the better. You must also continue to communicate clearly to your customers, taking care to avoid confusion with multiple messages that could change over time.

You should continue to consider what information consumers need to know and when. If customers need to act, then you must provide (or, in many cases, should have already provided) the information they need in a realistic time for them to make these decisions.

It's important you have answers ready to reassure customers where appropriate and make sure you're able to address customer queries accurately, fairly, clearly and promptly.

## Considerations for UK firms

If you're a UK-based firm and only do business in the UK, you're less likely to have been affected by the end of the transition period. You may not have been affected at all.

However, if you carried out business between the UK and the European Economic Area (EEA) – whether through a passport or directly under EU

legislation – you should have implemented plans to address any risks for your firm.

These questions will help you to decide whether you conducted business in the EEA and whether your business may have been affected by the end of the transition period.

- Did you provide any regulated products or services to customers resident in the EEA? For example, you might have provided financial advice to EEA-based customers. Or you might have had insurance contracts either with EEA-based customers or which covered risks located in the EEA that required regulatory permission in that country in order to be serviced.

- Did you have customers or counterparties based in the EEA, including UK expatriates now based in an EEA country?

- Did you market financial products in the EEA? This includes products marketed on a website aimed at consumers in the EEA.

- Did you have agents in the EEA or interact with any intermediary service providers in the EEA? For example, you may have used an insurance intermediary to distribute products into the EEA.

- Did your firm transfer personal data between the UK and the EEA or vice versa?

- Did your firm have membership of any market infrastructure (trading venues, clearing house, settlement facility) based in the EEA?

- Were you part of a wider corporate group based in the EEA, or did your firm receive any funding from an entity in the EEA?

- Did you outsource or delegate to an EEA firm or did an EEA firm outsource or delegate to you?

- Were you party to legal contracts which refered to EU law?

- Did you deposit client money and/or custody assets in any institution in the EEA, or was your safeguarding institution in the EEA?

If any of these questions apply to you – or you conducted (or currently conduct) business in the EEA in any other way – then you should think about the legal basis on which that business occured, and how that might have been affected by the end of the transition period.

This includes thinking about whether your firm needed additional regulatory permissions in the UK and/or in another country.

Not all these factors will automatically mean your business or your customers are impacted. There are other ways firms can access the EEA that may not be affected by the UK leaving the EU. However, these will depend on the specific firm, type of activity and the exemption or local permission in question.

These include:

- permission under local law or based on rules of a local financial market infrastructure

- local exemptions in an individual EEA country

- whether reverse solicitation is permitted without local authorisation – this is where the client initiates the provision of the service on their own initiative, and you do not promote or advertise services

- whether your activity would potentially be covered by any prospective EU equivalence decision on a specific aspect of the UK's regulatory framework.

*Number 3*

## ICO statement in response to UK Government's announcement on the extended period for personal data flows, that will allow time to complete the adequacy process

ICO is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

The Government has announced that the Treaty agreed with the EU will allow personal data to flow freely from the EU (and EEA) to the UK, until adequacy decisions have been adopted, for no more than six months. You may visit:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/948093/TCA_SUMMARY_PDF.pdf

This will enable businesses and public bodies across all sectors to continue to freely receive data from the EU (and EEA), including law enforcement agencies.

As a sensible precaution, before and during this period, the ICO recommends that businesses work with EU and EEA organisations who transfer personal data to them, to put in place alternative transfer mechanisms, to safeguard against any interruption to the free flow of EU to UK personal data. You may visit:
https://ico.org.uk/for-organisations/data-protection-at-the-end-of-the-transition-period/

As previously announced, the UK has, on a transitional basis, deemed the EU and EEA EFTA States to be adequate to allow for data flows from the UK.

Information Commissioner, Elizabeth Denham said:

“This is the best possible outcome for UK organisations processing personal data from the EU.”

“This means that organisations can be confident in the free flow of personal data from 1 January, without having to make any changes to their data protection practices.”

“We will be updating the ICO guidance on our website to reflect the extended provisions and ensure businesses know what happens next. At this stage it’s good news for businesses and public bodies.”


*Number 4*

## Financial Stability Oversight Council (FSOC), Annual Report

The U.S. economy was in the midst of the longest post-war economic expansion, with historically low levels of unemployment, prior to the onset of the COVID-19 pandemic earlier this year.

The global pandemic not only brought about a public health crisis but also caused a contraction of economic activity at an unprecedented pace.

Initially, the pandemic reduced consumer spending, slowed manufacturing production, and led to widespread business closures.

The unemployment rate surged from 3.5 percent in February to a record high of nearly 15 percent in April.

Since then, extraordinary measures undertaken by policymakers have succeeded in arresting the decline in economic conditions, initiating a recovery and lowering the unemployment rate to 7.9 percent as of September.

However, a protracted virus outbreak poses downside risks that can slow the recovery and even prolong the economic downturn.

## Financial Stress from the COVID-19 Pandemic and the Policy Response

The COVID-19 outbreak led to substantial financial stress in the first quarter of 2020.

While economic activity was disrupted in March, investors fled riskier assets for the safety and liquidity of cash and shortterm government securities.

A broad-based selloff in equities and commodities resulted in sharp declines in both spot and futures prices.

The sectors most affected by the pandemic, such as airlines, energy, transportation, hotels, and restaurants, recorded the sharpest declines.

The flight to safety and liquidity also created disruptions in short-term and global dollar funding markets.

Meanwhile, trading conditions for Treasuries and agency mortgagebacked securities (MBS), generally considered safe and liquid assets, were also strained.

Moreover, credit conditions tightened in the commercial paper (CP), corporate bond, and municipal debt markets.

With the stress in funding markets in March, precautionary draws by nonfinancial businesses on existing lines of credit with banks increased sharply, as firms tried to cover shortfalls in revenues and reductions in the availability of short-term funding.

Substantially increased liquidity and capital requirements imposed after the 2008 financial crisis helped banks meet the large, unanticipated drawdowns.

Large deposit inflows from investors fleeing to the safety of deposit insurance and borrowings at the Federal Reserve's discount window also helped in meeting this surge in liquidity demand.

Meanwhile, policymakers acted to minimize the health and economic effects of the pandemic.

On March 27, the Coronavirus Aid, Relief, and Economic Security (CARES) Act was signed into law.

The CARES Act authorized approximately $2.6 trillion in funding to address COVID-19 and to support the economy, households, businesses, and other entities.

In addition, the Federal Reserve and Treasury undertook a series of extraordinary measures beginning in March to contain the financial fallout from the pandemic.

The Federal Reserve also lowered the target federal funds rate to near zero and substantially increased purchases of Treasuries and agency MBS to ease trading pressures.

In a bid to stabilize short-term funding markets (STFMs), the Federal Reserve launched a series of facilities to provide liquidity to foreign central banks, primary dealers, depository institutions, and money market funds.

In light of these exigent circumstances, the Federal Reserve and Treasury also enacted a series of unprecedented measures to support corporate

bonds, bank loans, longer-term municipal debt, and asset-backed securities.

These credit and lending facilities were developed with the goal of relieving strains in longer-term debt markets through the pandemic.

These policy actions have substantially improved market conditions and investor sentiment in financial markets.

Federal Reserve purchases of Treasuries and agency MBS reduced bid-ask spreads and relieved the stress in trading conditions for these securities.

The announcement of liquidity facilities not only succeeded in lowering spreads on CP and short-term municipal securities but also reversed the heavy redemptions from prime and tax-exempt money funds.

The creation of new credit facilities lowered spreads on corporate bonds and revived new issuance in both the investment grade and high-yield bond segments.

Overall, these policy measures have restored the orderly functioning of financial markets and improved investor sentiment, as reflected in the rebound in corporate financing and equity prices.

The Council provided an important venue for facilitating coordination and analysis of risks across member agencies at the onset of the pandemic and throughout the year.

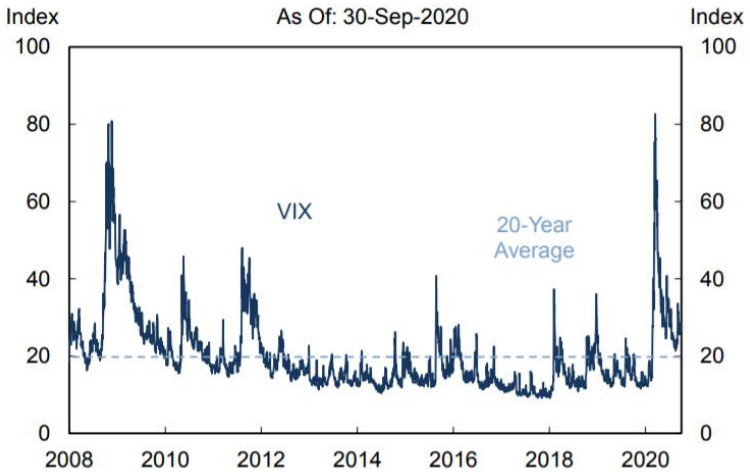
Council members regularly identified key risks and shared information regarding their policy responses.

The Council also increased the frequency of staff-level meetings to allow important analyses of major market developments to be shared in a timely manner with all Council member agencies.

In addition, the Council's previous identification of vulnerabilities and analysis that it had performed leading up to the financial stress helped ensure that policymakers' responses were more coordinated, well informed, and effective.

The report (216 pages):
https://home.treasury.gov/system/files/261/FSOC2020AnnualReport.pdf


### 3.2.2.1 S&P 500 Volatility




Source: Bloomberg, L.P.

*Number 5*

# OPINION ON THE 2020 REVIEW OF SOLVENCY II

*Legal basis*

1.1 On 1 January 2016, Directive 2009/138/EC of the European Parliament and of the Council on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II Directive) entered into application.

1.2 The Solvency II Directive provides that certain areas of the Directive should be reviewed by the European Commission (Commission) at the latest by 1 January 2021, namely:

• long-term guarantees measures and measures on equity risk,

• methods, assumptions and standard parameters used when calculating the Solvency Capital Requirement standard formula,

• Member States' rules and supervisory authorities' practices regarding the calculation of the Minimum Capital Requirement,

• group supervision and capital management within a group of insurance or reinsurance undertakings.

1.3 Article 77f(2) of the Solvency II Directive requires EIOPA to provide technical advice to the Commission in the form of an opinion on the assessment of the application of the long-term guarantees measures and measures on equity risk.

At the request of the Commission, the scope of EIOPA's Opinion is wider than that provided for in the Solvency II Directive.

1.4 EIOPA provides this Opinion to the Commission in accordance with Article 16a of Regulation (EU) No 1094/2010.

*Prudential context*

1.5 From a prudential perspective, the view of EIOPA is that overall the Solvency II framework is working well.

A risk-based approach to assess and mitigate risks is applied, the insurance industry has better aligned capital to the risks it runs, governance models

and their risk management capacity have been significantly strengthened, and insurers throughout Europe use harmonised templates for supervisory reporting, instead of a patchwork of national templates.

1.6 EIOPA's approach to the review overall has therefore been one of evolution rather than revolution. Thus, EIOPA's approach focuses on improving the existing regulation based on the prudential experience during the first years of application and taking into account the changes in the economic context.

In addition, the Commission in its request for advice from EIOPA sought that "the fundamental principles of the Solvency II Directive should not be questioned in the review".

*Economic context*

1.7 Nonetheless, from the perspective of the economic situation, there are areas of significant concern, which the review should address.

1.8 Subdued economic growth has led to extensive monetary easing and a general flight to safety.

This situation was further intensified by the Covid19 pandemic that has severely affected macroeconomic and market conditions worldwide. In October 2020, almost the entire euro swap curve moved to negative territory.

1.9 EIOPA's advice is that it is essential to recognise this economic picture in Solvency II.

Since its 2018 review of the Solvency Capital Requirement EIOPA has proposed changes to the treatment of interest rate risk in order to ensure that undertakings hold enough capital for that risk.

In addition, EIOPA recommends changes to the interest rate curves used by insurers to value liabilities, specifically in respect of the extrapolation of those curves.

The changes increase the influence of market interest rates on the extrapolation of the curves, making the liabilities more realistic and improving incentives for risk-management.

1.10 The recognition of the economic picture should reflect two aspects. Firstly, EIOPA's advice potentially sets the regulatory framework for a

decade and moreover any implementation of changes resulting from EIOPA's advice is likely to be closer to 2025 than to 2020.

Therefore, EIOPA considers it important that its advice, and its impact, not be unduly influenced by the point in time at which it is written particularly when that point may be atypical.

In light of this EIOPA recommends that the impact of the 2020 review should reflect the economic conditions as at end-2019.

1.11 Secondly, however, the impact of interest rates on insurers is expected to diminish over time reflecting a reduction in liabilities arising from products whose guarantees reflected the era of higher interest rates.

Low interest rates are mainly an issue with regard to the legacy book of insurance contracts.

Those insurance contracts are running off and their relevance for the overall portfolio will reduce over time. EIOPA therefore recommends that its proposal in relation to very low interest rates should likewise reduce over time.

1.12 EIOPA proposes a mechanism intended to reflect these circumstances. Specifically, the proposed new method of extrapolating the risk-free interest rates would have an "emergency brake" which would be applied when interest rate levels were below those of 2019.

The impact of the emergency brake should be temporary and phase out, reflecting the diminishing impact of the legacy book.

The mechanism is calibrated based on EIOPA's advice in all areas which have a material impact on the solvency position of insurers.

The advice on the mechanism should therefore be considered in conjunction with those other areas.

1.13 Regarding investments by insurers, since the introduction of the Solvency II framework the portfolio composition of European insurers has remained broadly stable.

In particular, fixed-income assets dominate the investment portfolios (almost two thirds of the investment portfolio), followed by equities (about 15% of the investment portfolio, including listed and unlisted).

Despite the negative yields experienced, insurers have continued to invest in negative or low yielding bonds. Moreover, this pattern was further strengthened due to flight-to-quality investment behaviour observed during the Covid-19 situation.

1.14 This behaviour is of wider concern in respect of the role of insurers as institutional investors.

Due to their long-term liabilities, life insurance companies in particular are well-suited to long-term investments.

EIOPA's advice is that there can be a more favourable but prudent treatment of insurers' long-term and illiquid liabilities, compared with those of shorter duration, recognising the extent to which such liabilities are predictable and stable.

This is reflected in EIOPA's advice regarding the volatility adjustment.

1.15 More favourable but prudent treatment is recommended for the equities which back long-term and illiquid liabilities.

Equity investments offer higher expected returns than fixed-income markets, but they also carry higher risk reflected in the higher volatility of their returns.

Though some empirical studies suggest that equities are less volatile in the longer-term, the EIOPA analysis did not support the current risk charge.

1.16 Under the Solvency II regulatory framework, the risk of insurers' equity investments is based on one year Value-at-Risk of the portfolio.

This approach reflects that a decrease in the market value of assets leads to a loss of own funds as an insurer could have to sell its assets at any time.

From a prudential perspective, it is important whether during periods of adverse market volatility an insurer is forced to sell its equities or whether it can hold on to them.

Equities which back long-term illiquid liabilities are more capable of being held on to, and therefore a more favourable prudential treatment is justified.

EIOPA's advice focuses on the criteria for the identification of longterm equities which back long-term illiquid liabilities.

To read more:
https://www.eiopa.europa.eu/sites/default/files/solvency_ii/eiopa-bos-20-749-opinion-2020-review-solvency-ii.pdf

**Contents**



*Number 6*

## Terrorist groups using COVID-19 to reinforce power and influence

INTERPOL

The impact of COVID-19 on global terrorism, trends and potential risks related to attacks on vulnerable targets and bioterrorism is the focus of a new report issued by INTERPOL.

LYON, France – The impact of COVID-19 on global terrorism, trends and potential risks related to attacks on vulnerable targets and bioterrorism is the focus of a new report issued by INTERPOL.

The assessment, which is for law enforcement use only, takes into consideration the following five main threat factors:

- COVID-19 outbreak characteristics and medical advances
- Global or national response
- Social climate
- Resilience of the security apparatus
- Strategies and capabilities of terrorists and other non-state actors (NSAs)

As COVID-19 cases subside in some regions and surge in others, the report underlines the critical need to monitor the reaction and response by terrorist networks, violent extremist groups, and other potentially dangerous NSAs.

*Economic impact*

Early in the pandemic, certain terrorist groups and other NSAs used the pandemic to reinforce their power and influence, particularly among local populations, or to expand their external financial resources.

The report also highlights how the impact of COVID-19 on the global economy is likely to indirectly affect funding available to terrorist organizations.

“Our terrorism assessment report is another tool to help law enforcement identify and address these evolving threats, in what continue to be challenging circumstances,” added Secretary General Stock.

The use of disinformation and conspiracy theories also appears as a common denominator across all idealistic spectrums, and as an indicator of prevailing threats against priority targets.

*Exploiting divisions*

The presence of far-right supporters in anti-COVID-19 activities in a growing number of western countries illustrates attempts to use the pandemic to exploit divisions. Law enforcement will continue to face attempts by far-right violent extremists to radicalize social movements, such as clashing with far-left groups and/or provoking the use of force.

Member countries are encouraged to exchange and crosscheck information related to individuals and groups using COVID-19 conspiracy theories to call and plan for violent acts. Coordinated and consistent use of INTERPOL Notices remain key to anticipate threats resulting from the direct and indirect impact of the pandemic.

The INTERPOL report also underscores how the recurring reinstatement of restrictive measures is likely to sustain a degree of civil unrest as well as impact on the choice of timing and targets for terrorist acts.

The report includes recommendations and early-warning signs for the global law enforcement community to monitor in addressing these threats.

To read more:
https://www.interpol.int/News-and-Events/News/2020/INTERPOL-Terrorist-groups-using-COVID-19-to-reinforce-power-and-influence

*Number 7*

## The Cybersecurity Strategy


The European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a new EU Cybersecurity Strategy.

The aim of this strategy is to bolster Europe's collective resilience against cyber threats and ensure that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools.

This includes the ever-increasing number of connected and automated objects in our homes, offices and factories.

The digital transformation of society, intensified by the COVID-19 crisis, has expanded the threat landscape and is bringing about new challenges, which require adapted and innovative responses.

The number of cyber-attacks continues to rise, with increasingly sophisticated attacks coming from a wide range of sources both inside and outside the EU.

The EU should therefore be leading the efforts for a secure digitalisation.

It should be driving norms for world-class solutions and standards of cybersecurity for essential services and critical infrastructures, as well as driving the development and application of new technologies.

Governments, businesses and citizens will all share a responsibility in ensuring a cyber-secure digital transformation.

*What is the strategy about?*

The strategy describes how the EU can harness and strengthen all its tools and resources to be technologically sovereign.

It also lays out how the EU can step up its cooperation with partners around the world who share our values of democracy, rule of law and human rights.

This technological sovereignty needs to be founded on the resilience of all connected services and products.

All the four cybercommunities – those concerned with the internal market, with law enforcement, diplomacy and defence – need to work more closely towards a shared awareness of threats.

They should be ready to respond collectively when an attack materializes, so that the EU can be greater than the sum of its parts.

The strategy covers the security of essential services such as hospitals, energy grids, railways and the ever-increasing number of connected objects in our homes, offices and factories.

The strategy aims to build collective capabilities to respond to major cyberattacks. It also outlines plans to work with partners around the world to ensure international security and stability in cyberspace.

Moreover, it outlines how a Joint Cyber Unit can ensure the most effective response to cyber threats using the collective resources and expertise available to Member States and the EU.

*Main aim of the strategy*

The new strategy aims to ensure a global and open Internet with strong safeguards where there are risks to security and the fundamental rights of people in Europe.

Following the progress achieved under the previous strategies, it contains concrete proposals for deploying three principal instruments.

These three instruments are regulatory, investment and policy initiatives.

They will address three areas of EU action:

- resilience, technological sovereignty and leadership;
- operational capacity to prevent, deter and respond;
- cooperation to advance a global and open cyberspace.

The EU is committed to supporting this strategy through an unprecedented level of investment in the EU's digital transition over the next seven years. This would quadruple previous levels of investment.

It demonstrates the EU’s commitment to its new technological and industrial policy and the recovery agenda. The EU’s new Cybersecurity Strategy for the Digital Decade forms a key component of Shaping Europe’s Digital Future, the Commission’s Recovery Plan for Europe and of the Security Union Strategy 2020-2025.

You may visit:
https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en

https://ec.europa.eu/info/strategy/recovery-plan-europe_en

https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en

https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade

*Number 8*

## Response to COVID-19 and medium- to long-term challenges for Japan's economy - with an eye on the post-COVID-19 era

Haruhiko Kuroda, Governor of the Bank of Japan, at the meeting of Councillors of Nippon Keidanren (Japan Business Federation), Tokyo.

*Introduction*

It is a great honor to have this opportunity to address such a distinguished gathering of business leaders in Japan today.

For eight years now, I have delivered a speech at this end-of-year meeting, and I can say that this year we have experienced enormous changes in the social and economic environment due to the shock of the novel coronavirus (COVID-19).

As we wrap up 2020, I would first like to take a look back at economic developments this year, mainly focusing on the impact of COVID-19, and talk about the outlook for economic activity and prices.

Then, I will explain the Bank of Japan's thinking behind its policy responses.

In relation to the conduct of monetary policy, I will also touch on the conduct of the assessment for further effective and sustainable monetary easing, which the Bank decided at the Monetary Policy Meeting (MPM) held last week.

Lastly, I would like to talk about what is necessary in taking advantage of lessons to be learned from overcoming the current crisis for future growth -- that is, challenges regarding Japan's economy as a whole that should be addressed when also looking ahead to the post-COVID-19 era from a medium- to long-term perspective.

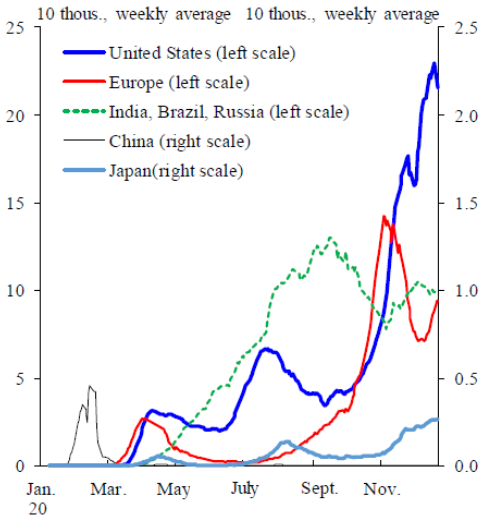
*I. Economic and Price Developments during the COVID-19 Era and Their Outlook Impact of COVID-19 on the Economy*

I. Economic and Price Developments during the COVID-19 Era and Their Outlook

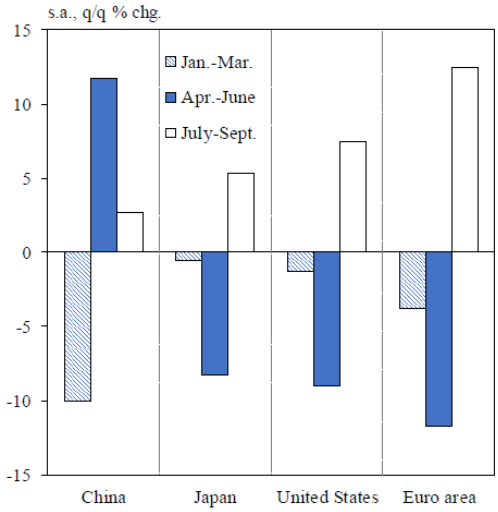
Chart 1

COVID-19

*Daily Confirmed New Cases*




*Major Economies' Real GDP (2020)*




Sources: Haver; OECD.

1

Let me start with a look back at economic developments this year, mainly focusing on the impact of COVID-19.

COVID-19 started to spread from the beginning of the year and became a pandemic within a short period toward early spring (Chart 1).

Governments around the world took strict and wide-ranging public health measures in order to prevent the spread.

Under these circumstances, the global economy became depressed significantly.

However, since the summer season, as public health measures have been eased, the global economy has picked up from that state of significant depression, as seen in the growth rates of each country turning positive on a quarter-on-quarter basis.

Similar developments have been observed in Japan.

The quarter-on-quarter GDP growth rate for the April-June quarter registered a considerably negative figure of minus 8.3 percent with wide-ranging economic activities being constrained.

However, that for the July-September quarter turned positive, to 5.3 percent, and Japan's economy has picked up from the bottom, although it has remained in a severe situation.

The economic fluctuation this time is different in nature from what was seen in the past.

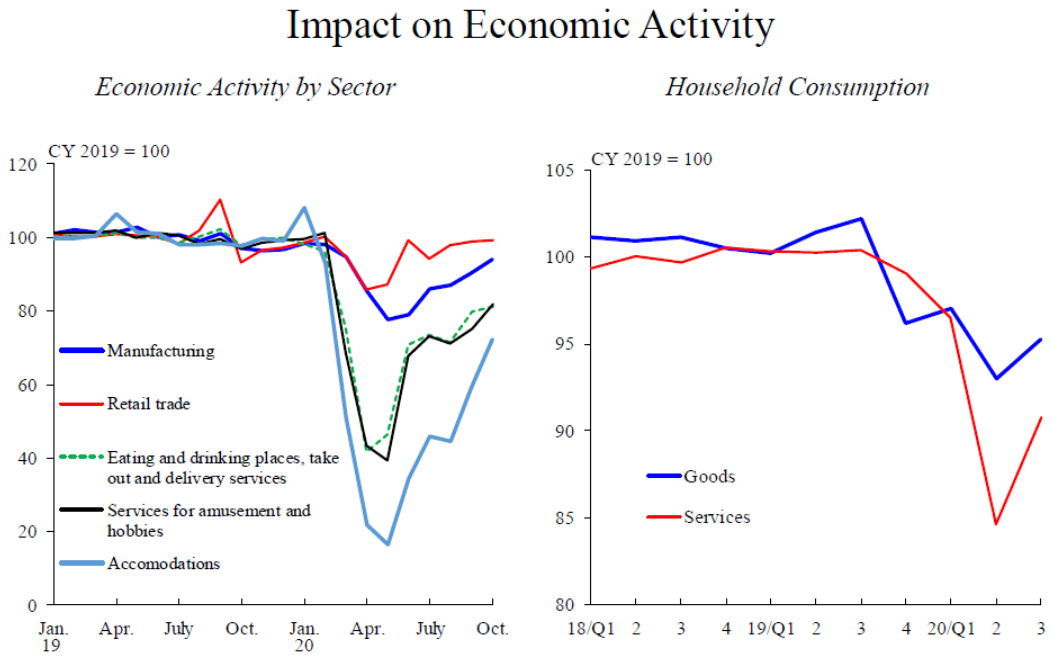
Most of the fluctuations since World War II were triggered by cyclical adjustments in business fixed investment and in inventory investment, or by financial imbalances.

On the other hand, the current fluctuation is exceptional, in that it stemmed from a shock caused by an infectious disease, which is not inherent in the economy, and that economic activity has been constrained exogenously with a view to preventing the spread of the disease.

In other words, such activity has been affected largely by an epidemiologic factor.

I. Economic and Price Developments during the COVID-19 Era and Their Outlook

Chart 2




Note: In the left-hand chart, figures for manufacturing are the "Indices of Industrial Production" and those for other sectors are the "Indices of Tertiary Industry Activity."
Sources: Ministry of Economy, Trade and Industry; Cabinet Office.

2

Reflecting the characteristics of COVID-19, economic activities that involve social interaction are particularly affected, and this is another point that is unique to the current case (Chart 2).

Looking at economic activities of firms in Japan by sector, a significant decline has been seen in the industry of face-to-face services such as eating and drinking as well as accommodations -- where firms are relatively small -- and amusement services including events.

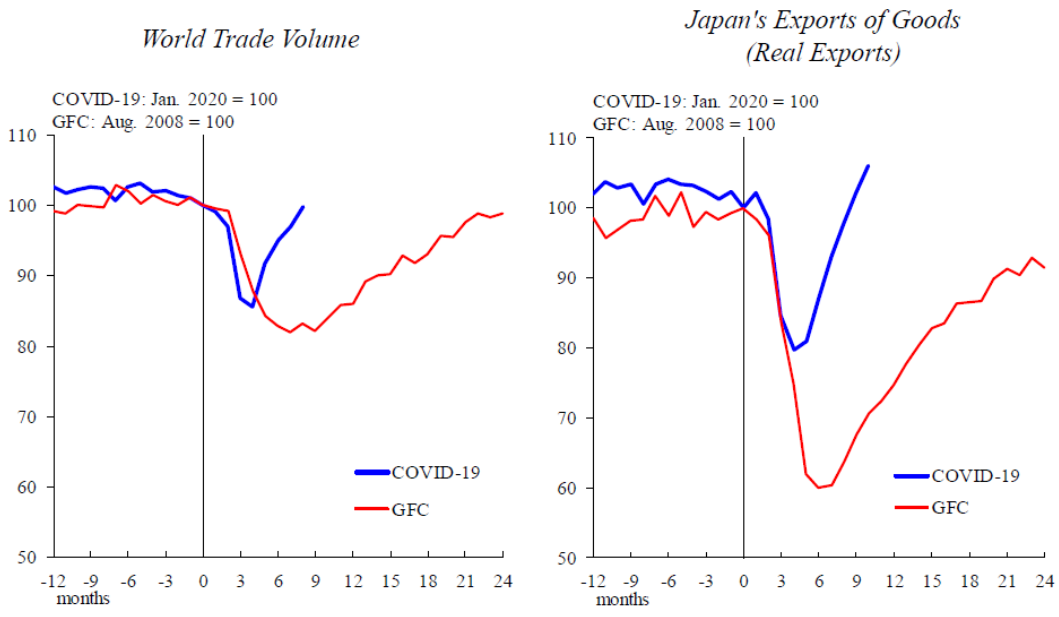
In terms of household spending, consumption of services has declined considerably compared with that of goods. A constraint on services consumption is due to vigilance against COVID-19, and the differences in consumption behavior of each age group reflect the degree of their vigilance.

That is, services consumption by the younger generation has recovered rapidly, whereas that by seniors, who are strongly vigilant against COVID-19, saw a significant decline and has picked up at a slower pace. In contrast, manufacturing and retail firms, which produce and sell goods, have been relatively less affected.

I. Economic and Price Developments during the COVID-19 Era and Their Outlook

Chart 3

Trade Activity of Goods




Sources: CPB Netherlands Bureau for Economic Policy Analysis; Bank of Japan; Ministry of Finance.

3

Goods transactions worldwide have picked up at a comparatively faster pace (Chart 3).

A decline in global trade activity has been small compared with at the time of Global Financial Crisis (GFC) and a rapid recovery has been observed. Under these circumstances, the level of Japan's exports has returned to that

seen prior to the COVID-19 outbreak, and at a rapid pace. This has led to manufacturers' relatively steady production activity.

As I have explained thus far, the impact of the shock of COVID-19 is uneven and largely varies for attributes such as the industry and size of firms as well as consumers' ages.

At the current phase in particular, this suggests the need to closely examine economic developments not only by looking at the aggregate or average values of data, but also through analyzing developments in different attributes of each economic entity.

To read more: https://www.bis.org/review/r201228a.pdf

*Number 9*

## Microsoft Internal Solorigate Investigation Update

Microsoft

As we said in our recent blog (https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/), we believe the Solorigate incident is an opportunity to work together in important ways, to share information, strengthen defenses and respond to attacks.

Like other SolarWinds customers, we have been actively looking for indicators of the Solorigate actor and want to share an update from our ongoing internal investigation.

Our investigation into our own environment has found **no evidence** of access to production services or customer data. The investigation, which is ongoing, has also found no indications that our systems were used to attack others.

As we previously reported, we detected malicious SolarWinds applications in our environment, which we isolated and removed. Having investigated further, we can now report that we have not found evidence of the common TTPs (tools, techniques and procedures) related to the abuse of forged SAML tokens against our corporate domains.

Our investigation has, however, revealed attempted activities beyond just the presence of malicious SolarWinds code in our environment. This activity has not put at risk the security of our services or any customer data, but we want to be transparent and share what we're learning as we combat what we believe is a very sophisticated nation-state actor.

We detected unusual activity with a small number of internal accounts and upon review, we discovered one account had been used to view source code in a number of source code repositories.

The account did not have permissions to modify any code or engineering systems and our investigation further confirmed no changes were made. These accounts were investigated and remediated.

At Microsoft, we have an inner source approach – the use of open source software development best practices and an open source-like culture – to making source code viewable within Microsoft.

This means we do not rely on the secrecy of source code for the security of products, and our threat models assume that attackers have knowledge of source code. So viewing source code isn't tied to elevation of risk.

As with many companies, we plan our security with an "assume breach" philosophy and layer in defense-in-depth protections and controls to stop attackers sooner when they do gain access.

We have found evidence of attempted activities which were thwarted by our protections, so we want to re-iterate the value of industry best practices such as outlined here, and implementing Privileged Access Workstations (PAW) as part of a strategy to protect privileged accounts.

We will provide additional updates if and when we discover new information to help inform and enable the community.

As we learn more from our own internal investigation, and from helping customers, we will continue to improve our security products and share these learnings with the community.

For the up-to-date information and guidance, please visit our resource center at https://aka.ms/solorigate

*Number 10*

## SolarWinds filing with the Securities and Exchange Commission

**CURRENT REPORT**

**PURSUANT TO SECTION 13 OR 15(d) OF**
**THE SECURITIES EXCHANGE ACT OF 1934**

**December 14, 2020**
**Date of Report (Date of earliest event reported)**

---

**SOLARWINDS CORPORATION**
**(Exact name of registrant as specified in its charter)**

SolarWinds Corporation ("SolarWinds" or the "Company") has been made aware of a cyberattack that inserted a vulnerability within its Orion monitoring products which, if present and activated, could potentially allow an attacker to compromise the server on which the Orion products run.

SolarWinds has been advised that this incident was likely the result of a highly sophisticated, targeted and manual supply chain attack by an outside nation state, but SolarWinds has not independently verified the identity of the attacker.

SolarWinds has retained third-party cybersecurity experts to assist in an investigation of these matters, including whether a vulnerability in the Orion monitoring products was exploited as a point of any infiltration of any customer systems, and in the development of appropriate mitigation and remediation plans.

SolarWinds is cooperating with the Federal Bureau of Investigation, the U.S. intelligence community, and other government agencies in investigations related to this incident.

Based on its investigation to date, SolarWinds has evidence that the vulnerability was inserted within the Orion products and existed in updates released between March and June 2020 (the "Relevant Period"), was introduced as a result of a compromise of the Orion software build system and was not present in the source code repository of the Orion products.

SolarWinds has taken steps to remediate the compromise of the Orion software build system and is investigating what additional steps, if any, should be taken.

SolarWinds is not currently aware that this vulnerability exists in any of its other products.

SolarWinds currently believes that:

• Orion products downloaded, implemented or updated during the Relevant Period contained the vulnerability;

• Orion products downloaded and implemented before the Relevant Period and not updated during the Relevant Period did not contain the vulnerability;

• Orion products downloaded and implemented after the Relevant Period did not contain the vulnerability; and

• Previously affected versions of the Orion products that were updated with a build released after the Relevant Period no longer contained the vulnerability; however, the server on which the affected Orion products ran may have been compromised during the period in which the vulnerability existed.

SolarWinds values the privacy and security of its over 300,000 customers and is working closely with customers of its Orion products to address this incident.

On December 13, 2020, SolarWinds delivered a communication to approximately 33,000 Orion product customers that were active maintenance customers during and after the Relevant Period.

SolarWinds currently believes the actual number of customers that may have had an installation of the Orion products that contained this vulnerability to be fewer than 18,000.

The communication to these customers contained mitigation steps, including making available a hotfix update to address this vulnerability in part and additional measures that customers could take to help secure their environments.

SolarWinds is also preparing a second hotfix update to further address the vulnerability, which SolarWinds currently expects to release on or prior to December 15, 2020.

For the nine months ended September 30, 2020, total revenue from the Orion products across all customers, including those who may have had an installation of the Orion products that contained this vulnerability, was approximately $343 million, or approximately 45% of total revenue.

There has been significant media coverage of attacks on U.S. governmental agencies and other companies, with many of those reports attributing those attacks to a vulnerability in the Orion products.

SolarWinds is still investigating whether, and to what extent, a vulnerability in the Orion products was successfully exploited in any of the reported attacks.

SolarWinds uses Microsoft Office 365 for its email and office productivity tools. SolarWinds was made aware of an attack vector that was used to compromise the Company's emails and may have provided access to other data contained in the Company's office productivity tools.

SolarWinds, in collaboration with Microsoft, has taken remediation steps to address the compromise and is investigating whether further remediation steps are required, over what period of time this compromise existed and whether this compromise is associated with the attack on its Orion software build system.

SolarWinds also is investigating in collaboration with Microsoft as to whether any customer, personnel or other data was exfiltrated as a result of this compromise but has uncovered no evidence at this time of any such exfiltration.

SolarWinds' investigations into these matters are preliminary and on-going, and SolarWinds is still discerning the implications of these security incidents. During the course of these investigations, SolarWinds may become aware of new or different information.

At this time, SolarWinds is unable to predict any potential financial, legal or reputational consequences to the Company resulting from this incident, including costs related thereto. So as not to compromise the integrity of any investigations, SolarWinds is unable to share additional information at this time.

To read more:
https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000162828020017451/swi-20201214.htm

## Disclaimer

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

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

This information:

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

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

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

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

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

- is in no way constitutive of an interpretative document;

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

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

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

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

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

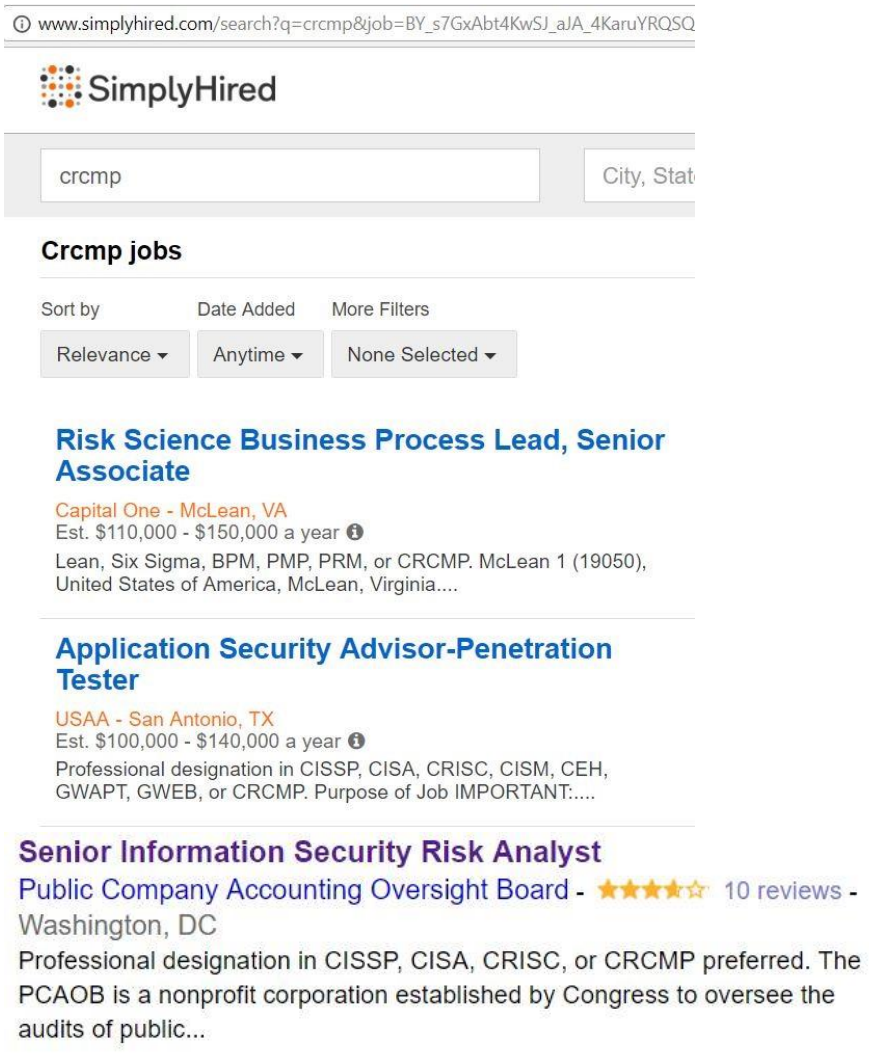
The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

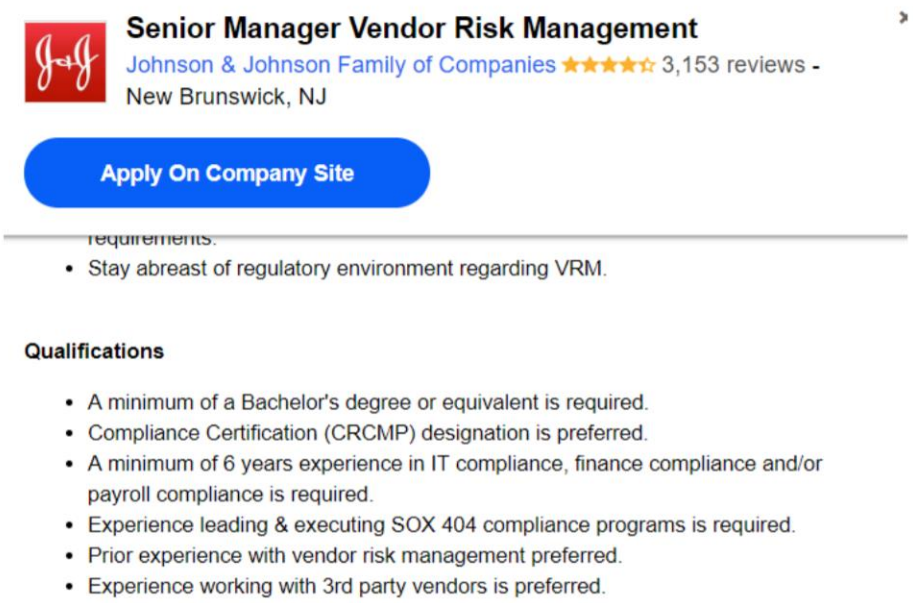
You can explore what we offer to our members:

1. *Membership* – Become a standard, premium or lifetime member.
You may visit:
https://www.risk-compliance-association.com/How_to_become_member.htm

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

3. *Training and Certification* – Become a Certified Risk and Compliance Management Professional (CRCMP), a Certified Information Systems Risk and Compliance Professional (CISRCP), a Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P, and / or a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I.





**Senior Manager Vendor Risk Management**

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

Apply On Company Site

requirements.

- Stay abreast of regulatory environment regarding VRM.

**Qualifications**

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

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

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

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

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

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

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

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