Financial Services Risk Trends

Covid | Compliance | Cyber | Culture | Climate Change | Claims

An Insurer's Perspective

Allianz Global Corporate & Specialty

About AGCS

Allianz Global Corporate & Specialty (AGCS) is a leading global corporate insurance carrier and a key business unit of Allianz Group. We provide risk consultancy, Property-Casualty insurance solutions and alternative risk transfer for a wide spectrum of commercial, corporate and specialty risks across 10 dedicated lines of business.

Our customers are as diverse as business can be, ranging from Fortune Global 500 companies to small businesses, and private individuals. Among them are not only the world's largest consumer brands, tech companies and the global aviation and shipping industry, but also satellite operators or Hollywood film productions. They all look to AGCS for smart answers to their largest and most complex risks in a dynamic, multinational business environment and trust us to deliver an outstanding claims experience.

Worldwide, AGCS operates with its own teams in 31 countries and through the Allianz Group network and partners in over 200 countries and territories, employing around 4,400 people. As one of the largest Property-Casualty units of Allianz Group, we are backed by strong and stable financial ratings. In 2020, AGCS generated a total of €9.3 billion gross premium globally.

www.agcs.allianz.com

The top five risks for the financial services sector as voted for by over 900 sector respondents in the **Allianz Risk Barometer 2021**

Overview

The financial services sector faces a period of heightened risks. Covid-19 has caused one of the largest ever shocks to the global economy, triggering unprecedented economic and fiscal stimulus and record levels of government debt. Despite an improved economic outlook, considerable uncertainty remains with regards to the course of the pandemic, while the effects of government and central bank responses are unpredictable. The threat of economic and market volatility lies ahead, as does the unprecedented challenge of returning workers to offices.

The specter of Covid-19 hangs over a sector already embarking on a major transformation, driven by fast-paced technology adoption and growing environmental, social and governance (ESG) issues. Climate change is having a significant impact, with a greening of investments and increased activism from environmental groups. International commitments to reduce greenhouse gases are giving rise to regulation, including potentially game changing ESG reporting and disclosure requirements.

Meanwhile, the behavior and culture of financial institutions is under growing scrutiny from a wide range of stakeholders in areas such as sustainability, employment practices, diversity and inclusion and executive pay. In an age of social media and increased disclosure, societal factors increasingly pose reputational risks for organizations and will influence regulation, litigation and liability for companies and directors.

An equally significant, if not greater, driver for risk going forward is the sector's growing reliance on technology and innovation. Covid-19 has only accelerated this, introducing new business models and ways of working. However, the move online is accompanied by an increase in risk exposure, driven by growing regulatory oversight in areas like data privacy, cyber security and business continuity. In future, the rollout of 5G, together with technologies like artificial intelligence and biometrics will bring new challenges in this area in addition to significant benefits.

Cyber and ESG issues only add to the challenging regulatory environment. Compliance issues are one of the biggest drivers of insurance claims for financial institutions with failings in governance and risk controls having brought large losses from a number of different areas.

These losses, compounded by Covid-19 uncertainty, have contributed to a recasting of the insurance market for financial institutions, characterized by adjusted pricing and greater risk selection by insurers, as well as a growing appreciation and interest in alternative risk transfer solutions.

Ultimately, financial institutions and their directors are having to navigate a rapidly changing world, and one in which risk management will increasingly need to focus on so-called "non-financial risks" and emerging societal trends. At the same time, technology-led business models will require greater attention on business resilience and the management of third-parties and supply chains.

This report highlights some of the most significant risk management trends currently occupying the attention of insurers, risk managers and broker partners in the sector, as ranked in the **Allianz Risk Barometer 2021**, which surveyed over 900 respondents. The aim is to start a dialogue around how they can best be managed.

In Brief:

- Large corrections or adjustments in markets – such as in equities, bonds or credit – could bring litigation from investors and shareholders.
- Directors and officers may be held accountable if there has been a failure to foresee or disclose Covid-19 related risks. Increased scrutiny around how companies prepare for future events.
- Rise in homeworking, fast adoption of new technologies, potentially weaker controls and oversight make companies/customers more vulnerable to cyber scams, and other internal/external crimes.
- Inadequate return to office plans could see employers face liabilities related to Covid-19 infections, employment practices and whistleblowing.

1 The Covid-19 risk landscape

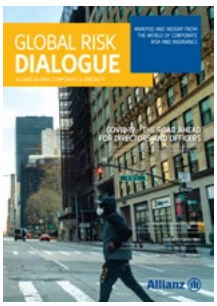
Despite an improving global outlook and the rollout of effective Covid-19 vaccinations, uncertainties surrounding the economic and financial market impact of the pandemic are the overriding concerns for financial institutions and their insurers.

Financial institutions are alive to the potential ramifications and unintended consequences of government and central bank responses to the pandemic, such as low interest rates, rising government debt and the winding down of support and grants and loans to businesses. Globally, governments have borrowed some $24trn during the pandemic, according to the **International Institute of Finance**[1], while in March 2021 the US announced a $1.9trn package, taking total US government pandemic spending to $6trn.

Such measures risk creating asset bubbles and stoke fears for inflation rises, which could cause losses further down the line. For insurers, this potentially creates a systemic risk in which losses impact multiple companies and sub-sectors simultaneously, around the world.

Large corrections or adjustments in markets – such as in equities, bonds or credit – could result in litigation from investors and shareholders, while an increase in insolvencies could also put some institutions' own balance sheets under additional strain. Indeed, **EU regulators**[2] warned in March 2021 of possible "further market corrections," saying that Covid-19 uncertainties weigh heavily on the prospects of a short-term economic recovery.

1 The Institute of International Finance, Global Debt Monitor, February 2021
2 EIOPA, EU financial regulators warn of expected deterioration of asset quality, March 2021



Find out more about how executives can manage Covid-19 related risks

Covid-19: Navigating the 'CEO moment' AGCS (allianz.com)

Covid-19 and the low interest rate environment is putting financial institutions under stress, explains **David Van den Berghe, Global Head of Financial Institutions at AGCS:** *"If there are bubbles in markets and values fall precipitously, it creates classes of unhappy customers and investors."*

Ultimately, Covid-19 could potentially generate claims across almost all lines of financial institutions insurance business. In particular, directors' and officers' insurance, professional indemnity, and errors' and omissions' insurance could see claims, but also potentially crime and cyber insurance.

Claims could be brought against directors and officers where there has been a failure to foresee or disclose Covid-19 related risks, or if sufficient steps were not taken to mitigate its impact. However, the threat of regulatory action and litigation related to Covid-19 is not limited to the start of the pandemic, says **Hannah Tindal, Head of Directors and Officers, UK, at AGCS**.

"Directors could be held to account for their actions at any point, including for the failure to put in place adequate risk controls, for example, following a switch to homeworking or a move to online services. Going forward, there will be ongoing questions around how companies prepare for future events, including potential further impacts of Covid-19," says Tindal.

What are the top five mega trends company directors and officers need to keep on top of during the year ahead?

Outlook:
Covid-19 and credit risk for banks

Banks have been assigned a key role in mitigating the economic shock from Covid-19 and supporting the recovery. This is in sharp contrast with the financial and debt crises a decade ago, which originated in the sector and saw banks reluctant to extend credit to protect their balance sheets, which in turn exacerbated the downturn. While the aftermath of those crises was characterized by a great deleveraging, Covid-19 led to a great re-leveraging, an explosion of debt.

*This is in large part the result of a somewhat "**Faustian Pact**,"* says **Ludovic Subran, Chief Economist at Allianz**. Policymakers have taken swift action to sweeten the deal for banks to ensure that they continue to provide an emergency liquidity lifeline to the private sector, despite rising credit risk. The measures range from central banks showering banks with new funding options and supervisors easing capital as well as liquidity requirements to national governments extending generous public guarantees to reduce direct exposure.

"Unprecedented policy support, however, may not be enough to shield European banks in particular. Amid the sharp economic downturn and the expected gradual recovery, non-performing loans (NPLs) are bound to increase notably. Are they prepared for the hit?" says Subran.

Pockets of vulnerabilities

Although capital ratios improved across the board in recent years, doubts remain as most banking sectors were already quite vulnerable before the onset of Covid-19, the result of more risk-taking in a decade-long historically low interest rate environment. Analysis by **Allianz Research** revealed various pockets of vulnerabilities that have emerged over the past few years in the Eurozone banking sectors in particular.

The French and Italian banking sector, for example, had the largest total amounts of NPLs in Europe. Turning to the NPL ratio, it was higher than the European Banking Authority indicative benchmark of 5% in Italy

continued on next page ↓

Increased risk of fraud and crime

The Covid-19 environment is providing fertile ground for criminals and fraudsters who are seeking to exploit the crisis. The combination of homeworking, fast adoption of new technologies, potentially weaker controls and oversight, as well as economic hardship, make companies and their customers more vulnerable to cyber-crime, investment scams, payment transfer and business email compromise fraud.

A survey of **fraud professionals**[3] found 77% had experienced an increase in fraud in 2020, while 92% expected a further rise in incidents through 2021. More than three-quarters indicated that preventing fraud is more challenging in the current environment. Cyber was seen as the most heightened risk, although bank fraud and employee embezzlement were expected to rise over the next 12 months.

"Employee fraud is a perennial exposure for financial institutions, and a risk that could be heightened if anti-fraud controls are compromised during the pandemic," says Van den Berghe. *"To date, Covid-19 has yet to result in a notable uptick in fidelity insurance claims, yet these typically increase in times of economic stress and hardship. Common features are weak controls and oversight at institutions, which enable rogue employees to steal funds or commit fraudulent acts undetected. At the same time, the risk of market abuse is also likely to be heightened, again due to remote working and reduced challenges."*

3 Association of Certified Fraud Examiners, Fraud In The Wake of Covid-19 Benchmarking Report, September 2020

and Portugal. Regarding the provisioning of NPLs, Dutch and British banks happened to have the weakest coverage of NPLs, exposing their banking systems to a sudden deterioration of asset quality.

On the other hand, German banks were by far the worst performer in terms of profitability and cost efficiency, despite the consolidation efforts of the sector. Return on equity (RoE) was also weak in Portugal, while Belgium stood out with weak cost-efficiency. Finally, banks in Portugal and Spain had the largest credit exposure to those sectors that are hit hardest by Covid-19, including accommodation and food service and art, entertainment and recreation.

"A deterioration of asset quality after Covid-19 seems inevitable," says Subran. *"It could easily impede banks' willingness and ability to lend to the economy, which in turn risks delaying the start of the new investment cycle."*

EU banks' profitability (RoE) tanked in the 12 months leading up to June 2020 dropping to 0.5% down from 7.0% as a result of a sharp rise in impairment costs. With structural headwinds firmly in place – in the context of a protracted low interest rate environment – revenues will remain under pressure in the coming years.

"To get Europe's banks back on a solid footing, it is high time to address the sector's underlying weaknesses by embracing efficiency and digitalization and pushing ahead with sector consolidation," says Subran.

*"In other words: '**The Faustian Pact**' of the pandemic has to be turned into something more sustainable. If, for example, Eurozone governments would double their efforts to complete the Capital Market Union as well as the Banking Union, it would go a long way to create a market environment for European banks in which they could strive and exploit economies of scale."*

Unprecedented risks of working with Covid-19

With the roll-out of Covid-19 vaccines, businesses will be planning for a return to the workplace in coming months. However, despite vaccinations, infection risks are likely to persist for some time yet, with the threat of new variants and the potential for a sizable unvaccinated population.

Vaccinations are likely to be key to financial services workers returning to offices. Businesses may require or encourage employees to get vaccinated in order to return or travel, while some institutions are going as far as to vaccinate employees. Allianz and Deutsche Bank, are among a number of **German companies** working with the government to vaccinate employees via in-house doctors.

Getting workers back into offices during a pandemic is a task without precedent for financial institutions, according to **Shanil Williams, Global Head of Financial Lines at AGCS**. *"This is likely to be a huge source of uncertainty, raising difficult questions around Covid-19 infection liability, vaccinations and privacy issues with regards to the medical information of employees,"* says Williams.

Employers will also need to consider the safety of unvaccinated staff and customers. Employment laws vary by region, however, employers could face liabilities related to Covid-19 infections, as well as those related to **employment practices and whistleblowing**. Whistleblower retaliation claims typically arise when employees raise health and safety concerns in the workplace.

Covid accelerates innovation and risk

Covid-19 is also making companies rethink business models, change ways of working and is accelerating adoption of new technology. The changes necessitated by the pandemic are unlikely to completely unwind once it subsides. For example, increased home-working and reduced levels of business travel (given companies' commitments to reduce greenhouse gas emissions) are likely to be maintained. Demand from consumers and businesses for online services is only likely to increase, resulting in reduced demand for office space and branches.

Across all sectors, the pandemic has accelerated digitalization by as much as seven years, according to a **McKinsey**[4] survey and such changes to ways of working and business models also have the potential for unintended consequences, says **Anton Lavrenko, Head of Financial Institutions, North America at AGCS**: *"For example, the increase in home working will have cyber security implications, as well as potentially increased compliance, conduct and employee wellbeing risks. Increased reliance on digitalization could bring increasing data protection and privacy risks and exposes around business continuity and business interruption, but also for financial crime and third-party liability."*

The pandemic has also reinforced societal changes. Employees returning to work after more than a year working from home are likely to have different views on work-life balance, and may demand more flexibility on when and where they work. For example, a recent survey of younger employees at one investment bank showed growing disquiet with working conditions – on average interns said they worked 95 hours per week. In the UK, mutual lender **Nationwide**[5] told its 13,000 staff they will be able to work from wherever they want in future.

4 McKinsey & Company, How Covid-19 has pushed companies over the technology tipping point - and transformed business forever, October 2020

5 Yahoo Finance, Nationwide says 13,000 staff can work from home even after the pandemic, March 2021

Outlook:
Impact of interest rates

Zero interest rates created big headaches for banks well before Covid-19. Besides the structural long-term effects – rising inequality, distorted financial markets and misallocation of resources – there were also direct income effects which are visible in the net interest income.

So far, these income effects have resulted in the "transfer" of billions of euros from private households to the state and corporate sector. The intermediating banks, too, have suffered in the process. As financial companies, mainly banks, boast both an asset-overhang and a positive interest rate differential they are the only sector with a positive net interest income. But since the financial crisis, it is in continuous decline, falling by €120bn to €450bn p.a. between 2008 to 2019 in the Eurozone. Cumulated changes amount to €865bn (8% of 2019 GDP). As assets outgrew liabilities, albeit by a relative small margin (2.8% p.a. vs. 2.2% p.a.), the main culprit was narrowing interest margins: while rates on received interest dropped by 294bp, rates on paid interest by "only" 270bp. The former might be attributable to the fact that banks piled into low-yielding assets such as sovereign bonds in recent years; the latter reflect the fact that banks usually enjoy the lowest rates of all sectors on their liabilities – the chunk of them being bank deposits – limiting the extent to which they can fall.

Covid-19 might have stopped the slide temporarily. When it hit the economy in 2020, banks provided the real economy with plenty of loans, satisfying corporates' hunger for cash. This was made possible by governments' generous support schemes and liquidity injections by central banks. The latter alone amounted to €1.8trn in 2020. *"From now on, however, the going will get (much) tougher. The outlook for loan growth and losses is less than rosy,"* says **Ludovic Subran, Chief Economist at Allianz.**

So far, guarantees and moratoria precluded the normal process that economic recessions lead to higher credit losses and non-performing loans. Support measures kept insolvencies artificially lower: defying

continued on next page ↓

economic logic, corporate insolvencies even declined by around 10% globally in 2020. In some European countries, the drop was even much larger. *"This scale of 'insolvency freezing' indicates the possible backlash: For most European countries, double-digit increases in insolvencies are on the cards for this or next year when these measures are gradually phased out,"* says Subran.

High stakes

The stakes are high: by the end of August 2020, guaranteed loans and loans under moratoria accounted for 7% and 15% respectively of the total stock of euro area corporate loans. *"With interest rates staying at rock bottom for the foreseeable future, the expected increase in credit losses, and tightening credit standards, it will become much harder for banks to compensate lower margins by higher lending volumes,"* says Subran. *"The decade-long slide in interest income could even accelerate after the short, pandemic-related reprieve."*

In future, this continued decline in revenues might weigh even more heavily on banks as other businesses become more contested, too. *"Covid-19 ushered in not only a new era of zero interest rates it also turbo-charged digitization in general and digital payments in particular. The cash-less society is no longer a wild dream. Even central banks have started to think seriously about introducing e-money,"* says Subran.

At this juncture, it is not clear which players might benefit the most from the cash-less economy. But competition in the business of payments will heat up, threatening banks to lose an important interface with clients, as they enter the race with a big handicap: Against the backdrop of structurally low profitability of the European banking sector, plagued by overcapacity, cost-cutting efforts could make it more difficult for banks to meet their digital transformation needs.

"Ironically, the onset of Covid-19 was a boon for banks' loan business, engineered by the massive interventions of governments and central banks. But this blessing in disguise is not meant to last. The aftermath of the pandemic will reveal the weak points of the sector with renewed brutality," says Subran.

In Brief:

- Growing numbers and new forms of financial crime, driven by Covid-19. At the beginning of the pandemic, the number of cyber-attacks rose by over 200%.
- Seismic shift in the regulatory view of privacy and cyber security. Cyber resilience and business continuity a growing area of focus.
- Third party service providers can be a weak link in the cyber security chain.
- Investing in training helps minimize the human error at the heart of most cyber incidents.

2 Cyber security concerns grow

Despite high levels of spending on cyber security, financial services companies remain an attractive target battling against a wide range of threats, including outright theft of funds, business-email compromise attacks, ATM "jackpotting", and extortion and ransomware attempts. Growing reliance on technology also means institutions face sizable business interruption exposures, as well as third party liabilities, when things go wrong.

Cyber security experts warned of a perfect storm for financial institutions as Covid-19 led to a rapid and largely unplanned increase in homeworking and electronic trading and this soon materialized. Attacks against the financial sector increased 238% globally from the beginning of February 2020 to the end of April, with some 80% of financial institutions reporting an increase in cyberattacks, according to cyber security firm **VMware**[1].

Recent months have also seen a number of major global cyber-attacks. In December 2020, the Orion system of information technology firm SolarWinds was compromised, affecting about 18,000 customers. In March 2021, Microsoft revealed that hackers were exploiting 'zero-day' vulnerabilities in its Exchange Server mail and calendar software to access company networks. The attacks see vulnerabilities in Microsoft Exchange servers being exploited to allow malicious code to be placed on them which can be used for ransomware, espionage or even misdirecting the system's resources to mine for cryptocurrency on behalf of the criminals.

Financial services companies continue to be heavily targeted, and typically feature in the top five sectors for severity and frequency of cyber-attacks, according to **Thomas Kang, Head of Cyber, Tech and Media, North America at AGCS:** *"These companies hold a lot of sensitive data on individuals, businesses and governments. At the end of the day, it is where the money is."*

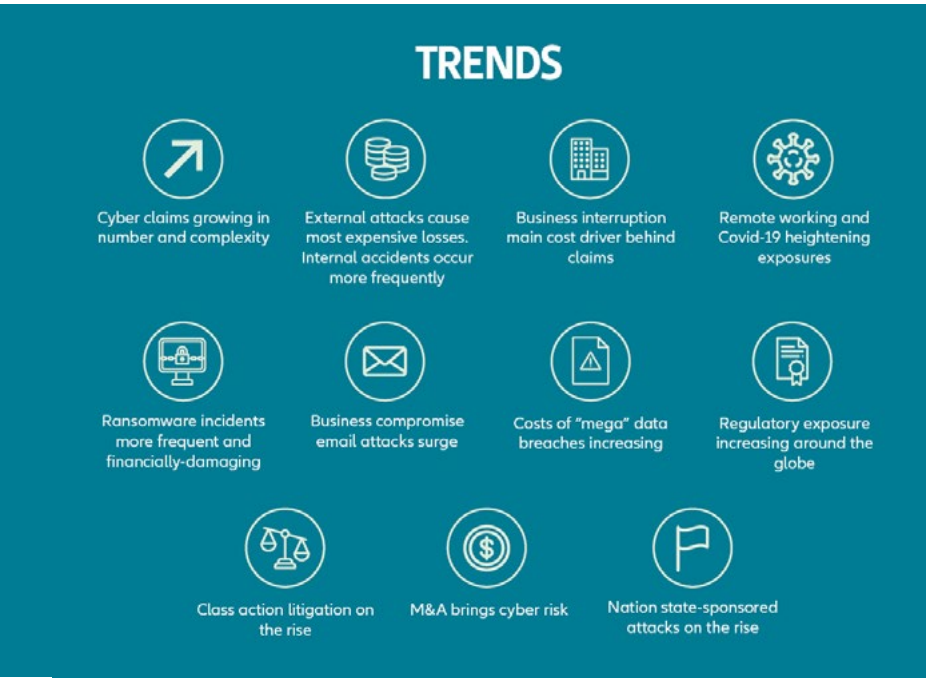
Cyber is an existential issue for financial institutions, which is why they invest heavily in cyber security, says Kang. However, with such potentially high rewards, cyber criminals will also invest time and money into attacking them. *"Take the Carbanak and Cobalt malware campaigns, for example. These* ***targeted***[2] *over 100 financial institutions in more than 40 countries over a five year period, stealing over $1bn,"* Kang adds.

1 VMware, 'Modern Bank Heists' Threat Report from VMware Carbon Black Finds Dramatic Increase in Cyberattacks Against Financial Institutions Amid COVID-19, May 2020
2 Europol, Mastermind Behind €1bn Cyber Bank Robbery Arrested In Spain, March 2018

Seismic shift in regulatory view of cyber security

At a time when financial institutions are becoming more reliant on technology and data to provide products and services to customers, they increasingly face a changing regulatory environment. In many parts of the world, financial services firms face a growing bank of regulation, including continually changing data protection and privacy rules, as well as cyber security requirements.

In particular, there has been a seismic shift in the regulatory view of privacy and cyber security, explains Kang: *"Where regulators previously looked to incentivize firms to invest in cyber security, they now see it through the lens of consumer rights and data privacy. With the General Data Protection Regulations (GDPR) in Europe and the California Consumer Privacy Act, companies now need to operationalize their response to regulation and privacy rights, not just look at cyber security."*



The consequences of data breaches are increasing, with more aggressive enforcement, higher fines and regulatory costs, and growing third party liability. Under the GDPR, the number and value of fines for data and privacy has been growing while jurisdictions around the world have been introducing stricter data laws. Increasingly, breaches and regulatory actions are followed by litigation, with a number of group actions now pending in the UK as well as the US. A data breach at Capital One bank in 2019 – one of the largest-ever – resulted in an $80m fine[3] and a number of lawsuits by affected customers. More recently, regulators have turned their attention to cyber resilience and business continuity. Following a number of major outages at banks and payment processing companies, regulators have begun drafting business continuity requirements in a bid to bolster resilience.

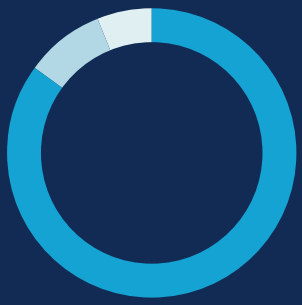
In October, 2020, a technical glitch halted trading on Japan's stock exchanges, while, a couple of months earlier, the New Zealand Stock Exchange shut down operations after a network provider experienced an extended distributed denial of service (DDoS) attack. These incidents came just months after a ransomware attack caused almost a month of outages at foreign exchange company Travelex, which also affected services at a number of banks.

In the UK, the Financial Conduct Authority (FCA) recently introduced rules and guidance on operational resilience for banks and insurers. The rules, which will come into force on March 31, 2022, require firms to address disruption to important business services from a range of events, including a cyber-attack, technical glitches and power outages. In Europe, the proposed Digital Operational Resilience Act (DORA) would introduce an EU-wide regulatory framework on digital operational resilience for a wide range of financial services firms, with a focus on business continuity and the management of third-party risk.

3 Reuters, Capital One to pay $80mn fine after data breach, August 2020

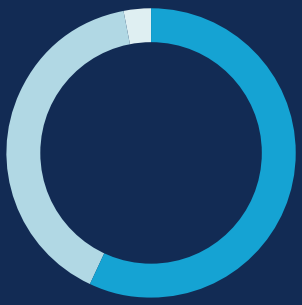
Where do cyber claims come from?

Cause of loss by value of claims



- **External manipulation of systems** (e.g. direct attack from the internet or malicious content such as ransomware/malware) **85%**
- **Malicious internal action** (e.g. action taken by a rogue employee) **9%**
- **Accidental internal cause** (e.g. human error, technical/systems failure or outage) **6%**

Cause of loss by number of claims



- **Accidental internal cause** (e.g. human error, technical/systems failure or outage) **57%**
- **External manipulation of systems** (e.g. direct attack from the internet or malicious content such as ransomware/malware) **40%**
- **Malicious internal action** (e.g. action taken by a rogue employee) **3%**

Based on the analysis of 1,879 claims worth €673mn ($812mn) reported from 2015 until year-end 2020. Total includes the share of other insurers involved in the claim in addition to AGCS.
Source: Allianz Global Corporate & Specialty

Losses resulting from the external manipulation of computers such as distributed denial of service attacks (DDoS) or phishing and malware/ ransomware campaigns account for the significant majority of the value of claims analyzed across all industry sectors (not just involving financial services companies). Cyber-crime generates the headlines, but the analysis shows that more mundane technical failures, IT glitches or human error incidents are the most frequent generator of claims, although, overall, the financial impact of these is limited.

Whether it results from an external cyber-attack, human error or technical failure, business interruption is the main cost driver behind cyber claims. It accounts for around 60% of the value of all claims analyzed.

Find out more about trends in cyber risk

Cyber risk trends 2020 AGCS

Ransomware one of the most prominent threats

Ransomware attacks continue to increase in frequency and severity, with ever larger ransom demands. Last year, the Securities Exchange Commission in the US **warned** about a rise in the number and sophistication of ransomware attacks on US financial institutions. Ransomware attacks were up nine fold between February and end of April 2020, according to **VMware**.

A recent development has seen hackers steal sensitive data and threaten to publish it online if ransoms are not paid. US lender **Flagstar Bank**, for example, suffered a ransomware attack in early 2020 that saw hackers post personal details online in an attempt to extort money. Last year, Chilean bank BancoEstado shut down branches after a ransomware attack.

"We have seen an increased frequency of these attacks in the past year," says **Marek Stanislawski, Global Cyber Underwriting Lead at AGCS**. *"If criminals can get access to critical systems or sensitive data they will look to monetize the attack through extortion. At the same time, the rise of cryptocurrencies like Bitcoin is making it easier for cyber criminals to carry out successful ransomware or extortion attacks."*

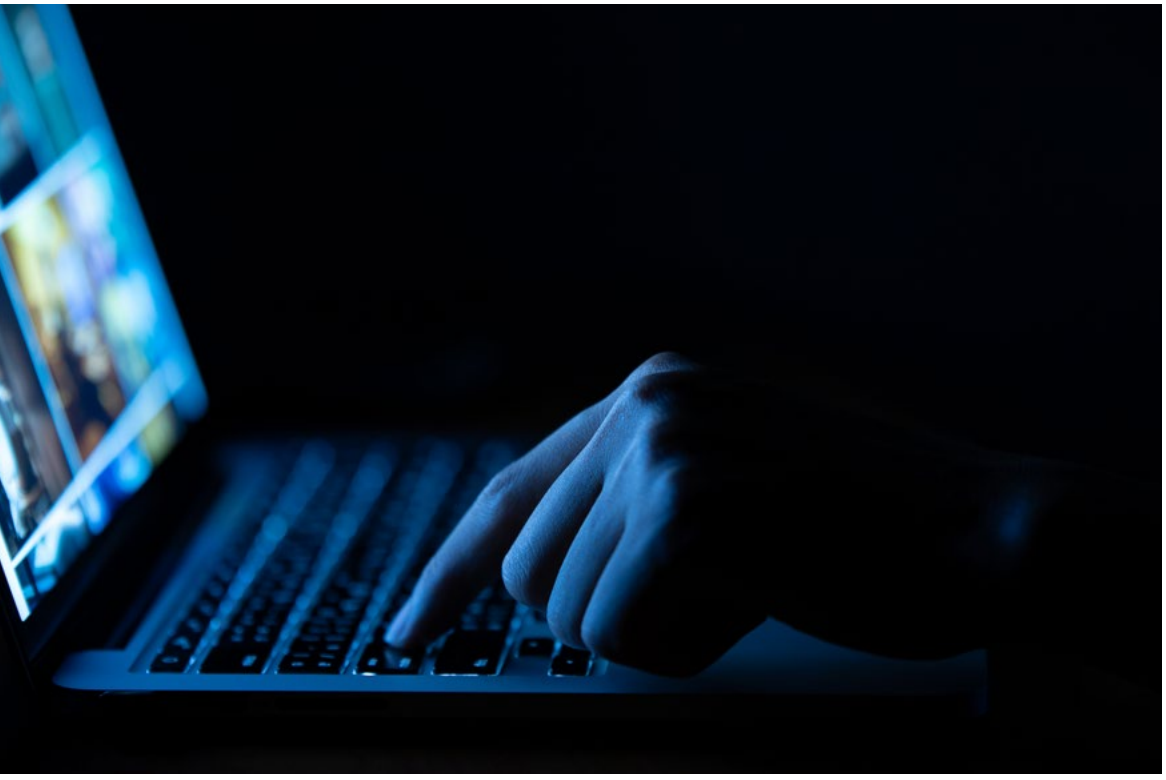
In March 2021, CNA Hardy was also hit by a sophisticated ransomware attack which impacted its operations and email systems and significantly disrupted the insurer for a number of weeks.

Rising cyber scams – "Fake presidents" and ATM "Jackpotting"

With many employees working from home and under increased stress, Covid-19 has created opportunities for cyber criminals to carry out various scams and cyber-attacks. The US Federal Bureau of Investigation (**FBI**[4]) received over 28,500 complaints related to Covid-19 cyber-crime alone in 2020. Many incidents looked to exploit stimulus funds and Paycheck Protection Program (PPP) loans, as well as to use Covid-19 related phishing attacks to steal money or personal data.

Business email compromise (BEC) attacks, also known as "fake president" attacks, are a particular problem for financial institutions that make large numbers of high value payments on behalf of their customers. The cost of BEC attacks reached $1.86bn in 2020, accounting for almost half of all reported cybercrime losses. Such attacks are becoming more sophisticated and increasingly involve identity theft and funds being converted to cryptocurrency.

ATM "jackpotting" attacks continue to be a threat. In July 13, 2020, a Belgian savings bank Argenta shut down 143 cash machines after criminals tried to take control of their cash machines through their network servers. These attacks have become increasingly sophisticated and over the last five years, jackpotting has cost the financial services sector millions of dollars: the Ploutus family of ATM malware, which originally appeared in Mexico in 2013, has created losses of over $450mn around the world.



4 FBI, Internet Crime Report 2020

Cloud and supply chains bring challenges as well as opportunities

Find out more about cyber security best practice for employees when working remotely

Coronavirus: Fighting the rise in cyber criminals from the home office | AGCS

One of the largest and most sophisticated attacks of the past year, the SolarWinds incident, was a supply chain attack. Hackers accessed SolarWinds' network and injected malware into its management software in order to target thousands of organizations, **including banks** and agencies.

The SolarWinds breach is an **important reminder** of the potential vulnerabilities of the financial services sector to cyber-attacks and outages via their reliance on third-party suppliers and service providers, over which they have little or no control when it comes to cyber security. This is likely to become a bigger issue as regulators increasingly focus on business continuity and operational resilience going forward.

"Third-party service providers can be the weak link in the cyber security chain," says Kang. *"We recently had a bank client suffer a large data breach after a third-party vendor failed to delete personal information when decommissioning hardware."*

Most financial institutions are now making use of cloud services-run software to access additional processing capacity, as well as for IT infrastructure or to carry out certain processes, such as fraud detection or analytics. However, the transition to cloud services has pros and cons. On the one hand, cloud providers are developing tools to help organizations manage and mitigate their cyber risks, yet a growing reliance on a relatively small number of cloud providers, and an opaque cloud infrastructure, is creating potentially large and systemic risks. A survey of banks and insurers by the Bank of England[5] last year found the provision of IT infrastructure in the cloud is already highly concentrated – the top two infrastructure-as-a-service providers had around two-thirds market share for banks.

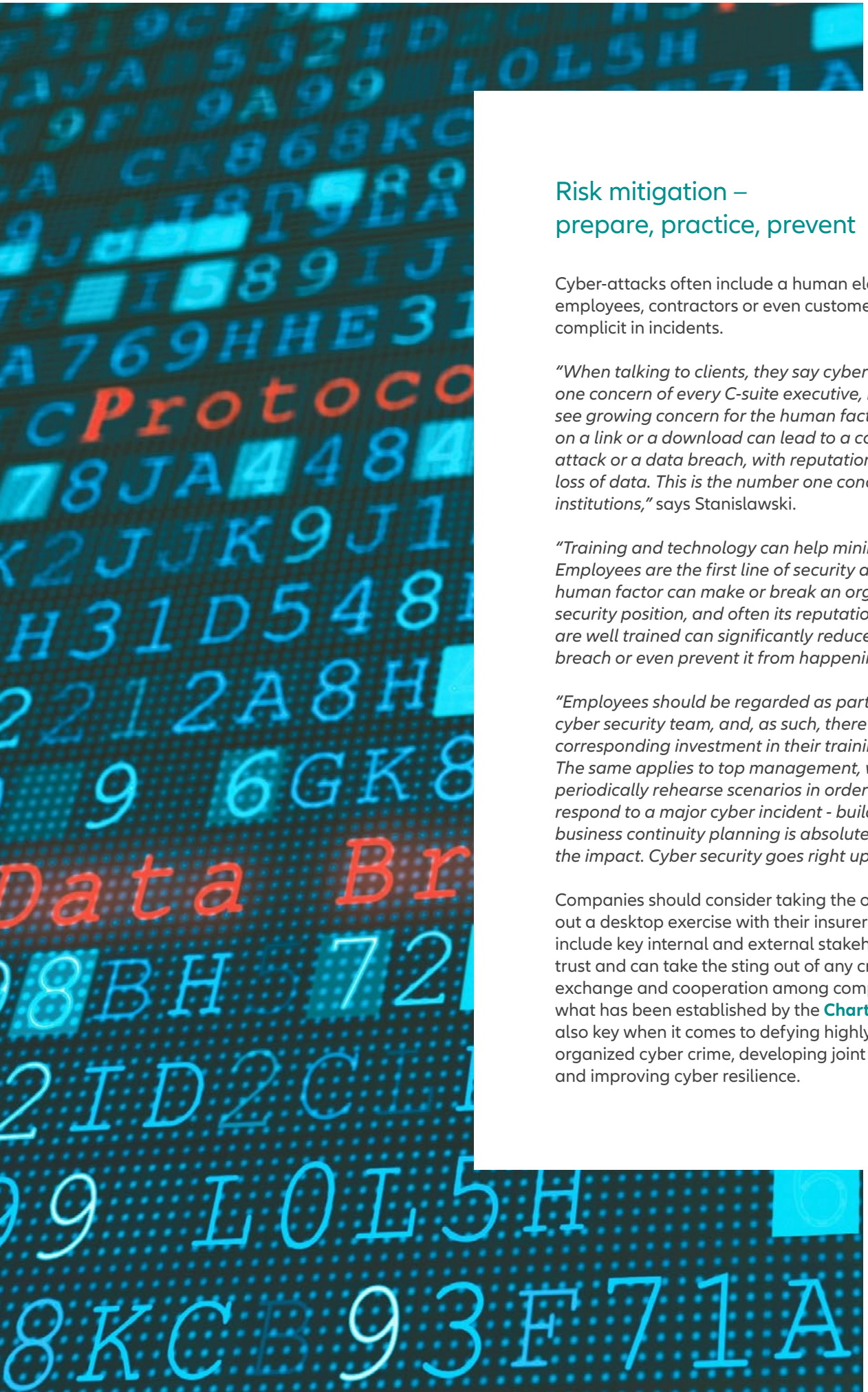
The move to the cloud raises questions around managing risks and liability, according to Kang. *"How financial institutions manage risks presented by the cloud will be critical going forward. They are effectively offloading a significant portion of cyber security responsibilities to a third-party environment. Your cloud service vendors become your exposure. However, by partnering with the right cloud service provider, companies can also leverage the cloud as a way to manage their overall cyber exposure."*

5 Bank of England, How reliant are banks and insurers on cloud outsourcing? January 2020

New cyber risk management solution for the cloud

Companies are increasingly using cloud-based solutions: according to **Gartner Research**. By 2024, more than 45% of IT spending will shift from traditional solutions to the cloud. Cloud usage comes with many benefits, such as lowered cost, enhanced data analytics and expanded collaboration, but also new potential risks around security, compliance and data privacy, especially for those in heavily regulated markets such as financial services and healthcare.

AGCS and Munich Re have recently developed a new commercial cyber risk insurance solution called **Cloud Protection +**, designed for customers of Google Cloud enrolled in Google's new "Risk Protection Program." The Risk Protection Program consists of two components: Risk Manager, a new tool that helps determine a customer's security risk posture on the cloud, and **Cloud Protection +** – a new cyber insurance solution built for Google Cloud customers. Under **Cloud Protection +**, companies are offered, subject to underwriting eligibility, protection against cyber incidents within their own corporate environment as well as incidents related to Google Cloud. Customers are US-based at present, although it may be offered globally in future.



Risk mitigation – prepare, practice, prevent

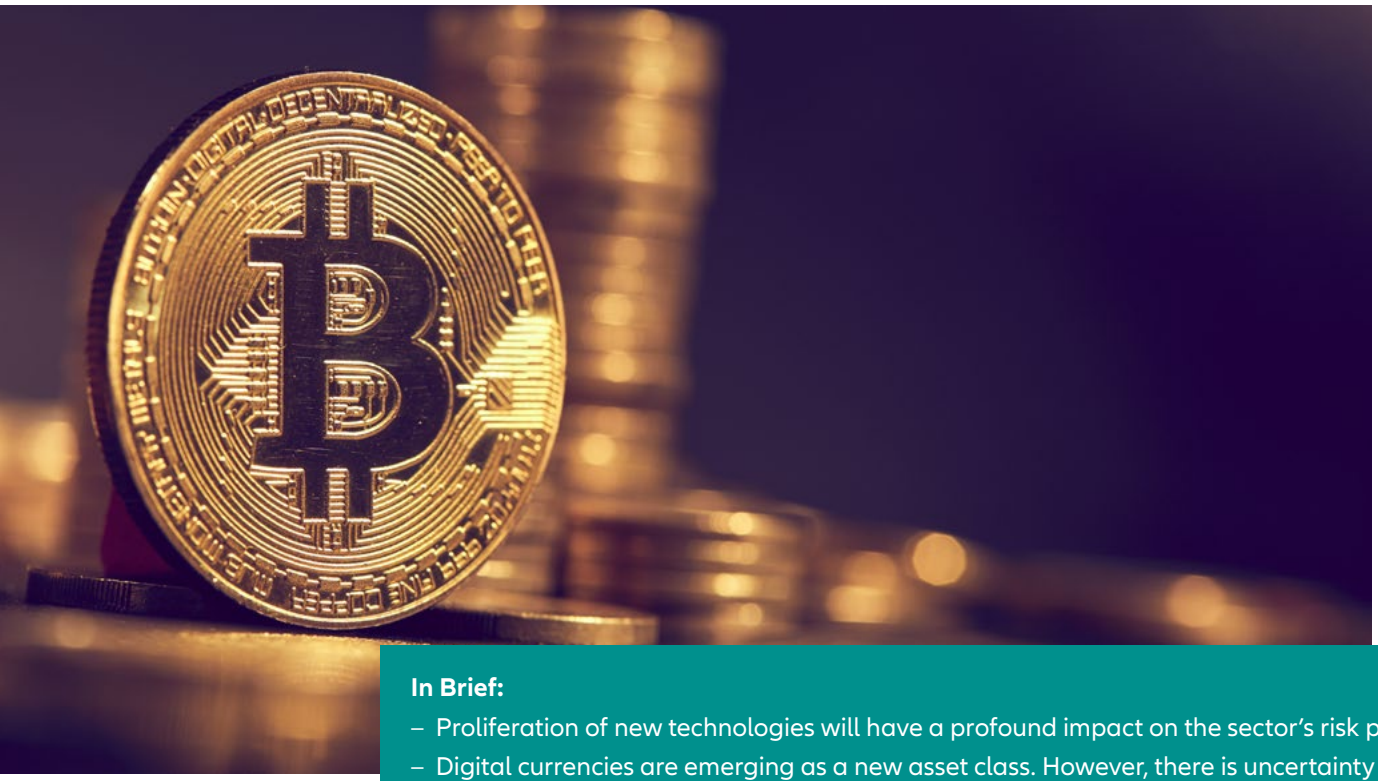
Cyber-attacks often include a human element, where employees, contractors or even customers are unwittingly complicit in incidents.

"When talking to clients, they say cyber is the number one concern of every C-suite executive, in particular we see growing concern for the human factor. Just one click on a link or a download can lead to a costly ransomware attack or a data breach, with reputational damage and loss of data. This is the number one concern for financial institutions," says Stanislawski.

"Training and technology can help minimize human error. Employees are the first line of security and defense. The human factor can make or break an organization's cyber security position, and often its reputation. Those that are well trained can significantly reduce the impact of a breach or even prevent it from happening.

"Employees should be regarded as part of the cyber security team, and, as such, there should be a corresponding investment in their training and education. The same applies to top management, who should periodically rehearse scenarios in order to prepare and respond to a major cyber incident - building resilience and business continuity planning is absolutely key to reducing the impact. Cyber security goes right up the chain."

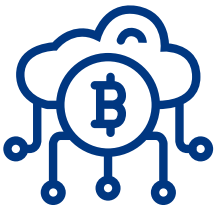
Companies should consider taking the opportunity to carry out a desktop exercise with their insurer and broker, and include key internal and external stakeholders. This builds trust and can take the sting out of any crisis. Cross-sector exchange and cooperation among companies – such as what has been established by the **Charter of Trust** – is also key when it comes to defying highly commercially-organized cyber crime, developing joint security standards and improving cyber resilience.



In Brief:

- Proliferation of new technologies will have a profound impact on the sector's risk profile.
- Digital currencies are emerging as a new asset class. However, there is uncertainty around potential asset bubbles and regulation and concerns about money laundering, ransomware attacks, third party liabilities and ESG issues.
- Growth in stock market investing by small investors guided by social media, raises mis-selling concerns.

3 Unintended consequences of innovation and new technologies



The increasing digitalization of financial services brings many benefits but also potential new risks and liabilities for the sector as it moves to a technology-driven model, with virtual currencies, artificial intelligence (AI) and biometrics.

The lines between financial institutions and technology companies are blurring, and in some cases even merging. Technology companies are moving into financial services – the likes of Apple, Google and Amazon are offering or developing banking and other financial services, while Facebook is launching its own virtual currency, Libra. The FinTech sector continues its rapid ascent, while incumbents are partnering with technology firms to enhance their offerings and improve efficiency. Cloud computing and AI-powered robotics are being used to automate processes, carry out analysis and make decisions, while connected devices and biometrics can collect a wealth of information on a customer's health or behavior.

The proliferation of new technologies in financial institutions, in particular AI, robotics and biometrics, will have a profound effect on the sector's risk profile. On the one-hand, new technology applications can be a positive for risk management, such as where they improve security, compliance controls, or encourage customers to improve their risks, but they also can bring potentially new or little understood exposures, according to **Shanil Williams, Global Head of Financial Lines at AGCS**.

Every time a new technology is developed or applied, it can creates risks and unintended consequences, adds **Marek Stanislawski, Global Cyber Underwriting Lead at AGCS**: *"With each new technology, we move the goalposts and potentially increase the attack surface for cyber criminals. For example, there are a lot of potential benefits to digital and virtual currencies, but they also can help fuel cybercrime, extortion and ransomware."*

The rollout of 5G technology, in particular, has the potential to change the risk landscape. *"This is not just about new technologies, like AI and machine learning,"* says **Thomas Kang, Head of Cyber, Tech and Media, North America at AGCS**. *"With 5G, there will be an explosion of data availability, which can power AI, but the implications are not yet well understood, and there will be new risks from a policy and regulatory perspective.*

"We are approaching a threshold as more and more connected devices create huge amounts of data on individuals' health, behavior and preferences. Such data creates opportunities for financial institutions, but if its use is not always well thought through and tested, it may fall foul of privacy statutes, like the EU's General Data Protection Regulations."

Increasing use of technology and data needs to considered against the backdrop of developing data protection and privacy regulations.

"Technology is evolving light years ahead of policy and regulation. Regulations in this area are continually changing – for example, notification and privacy laws are being updated in the US and many other countries – but we probably do not yet have the extent of regulation that we will need, especially in specific areas like biometrics or 'know your customer' rules [for cryptocurrencies]," says Kang.

The applications of new technologies such as AI, biometrics and virtual currencies will likely raise new risks and liabilities in future, in large part from compliance and regulation.

With AI, we already have seen the risks of unconscious bias, resulting in regulatory investigations in the US related to the use of **algorithms** for credit scoring. There have also been a number of lawsuits in the US related to the collection and use of biometric **data**.

Cryptocurrencies raise concerns

The growing acceptance of digital or cryptocurrencies will ultimately present operational and regulatory risks for financial intuitions.

The value of **bitcoin has surged** during the pandemic, up over 100% in the first three months of 2021, with the total cryptocurrency market valued at almost **$1.5trn**[1]. According to **Deutsche Bank**[2], bitcoin is now the third-largest currency in terms of the total value in circulation. Digital currencies are also gradually making their way into the real world. In February, Tesla announced that it had purchased $1.5bn worth of bitcoin, and that it would start accepting it as a payment method for its **vehicles**. Last year PayPal announced it would allow customers to buy, sell and hold virtual assets, including bitcoin.

The worlds of digital currencies and traditional financing are beginning to merge, according to Williams. *"Digital currencies are emerging as a new asset class, and we are starting to see traditional investors and banks get more involved. However, crypto-currencies are surrounded by uncertainty, with questions around potential asset bubbles and regulation, as well as concerns for potential money laundering and the risks of theft or loss of access. There are even potential environmental, social and governance (ESG) issues, as 'mining' or creating cryptocurrencies uses large amounts of energy,"* says Williams.

Companies involved in the trading, mining, processing and storage of digital assets will increasingly face a number of potential liability and regulatory exposures. Central banks and financial regulators are turning their attention to digital currencies, which are seen as an opportunity, as well as a threat. **India**, for example, recently announced it would require companies to disclose their crypto holdings to the government as part of their financial statements.

"Financial institutions that facilitate the trading and processing of virtual assets or take custody of cryptocurrencies will face the prospect of potential third party liabilities," says Williams. "There is a lot of debate around cryptocurrencies in the market, and there have already been losses in the sector from theft, fraud and lost coins and keys."

Cryptocurrencies also come with compliance risk, in particular with respect to anti-money laundering requirements and sanctions rules that prohibit facilitating payments to terrorist groups, criminals or sanctioned individuals or organizations.

"As banks dive deeper into crypto and digital currencies, 'know your customer' processes become even more important," says Kang.

1 Reuters, Analysis: Biden's SEC chair nominee signals more regulation for cryptocurrencies, March 2021
2 Deutsche Bank, Bitcoins: Can the Tinkerbell Effect Become a Self-Fulfilling Prophecy?, March 2021

Gamestop – the rise of meme stocks

Growth in stock market investing by small investors guided by social media raises issues for financial institutions and regulators around market volatility and consumer-facing compliance.

In the early months of 2021, struggling Texas-based video game retailer GameStop became the center of a battle between small traders, using social media forums such as Reddit, and more established institutional investors and hedge funds. Buying shares en masse, the activist retail investors drove GameStop's share price to a high of $483 in February, up from just $3.25 a share the year before.

Trading in 'meme' stocks like GameStop – which gain favor in online platforms – have stoked fears of stock market volatility and unpredictability driven by social media and activist retail investors. According to **Bloomberg**, 50 meme stocks added $276bn in value from the end of 2020. However, in just a matter of days, 60% of that value had been wiped out.

Regulators are already expressing concern for the effects of social media on stock market volatility and the impact on small investors. The Securities Exchange Commission **(SEC), for example**, has **suspended trading** on a number of meme stocks inflated by social media discussion groups, while the **Financial Industry Regulatory Authority** is reportedly investigating the social media activity of stockbrokers following the GameStop trading frenzy.

The lessons of GameStop have wider implications for the role of social media in financial investments. A study from the UK's **Financial Conduct Authority** (FCA) found that a new, younger, more diverse group of consumers are getting involved in higher risk investments, potentially prompted in part by the accessibility offered by new investment apps, social media and online advertising. It says it is worried that some investors are being tempted – often through online advertisements or high-pressure sales tactics – into buying higher-risk products that are very unlikely to be suitable for them.

In Brief:

- Only a third of companies consider themselves to be very effective at managing ESG risk.
- Surge in ESG regulations and guidance means tougher disclosure and reporting requirements for companies.
- Litigation or investor, shareholder and activist actions increasingly focus on ESG topics such as climate change, pollution, diversity and even CEO pay.
- Elevating and identifying ESG risks through a business' risk registers and committees, and making sure it is understood how they will play out in and out of the boardroom, is crucial.

4 ESG factors take center stage

With growing concern for the impacts of climate change risk and social inequalities, environmental, social and governance (ESG) risks are receiving greater attention from financial institutions, investors and regulators.

Financial institutions and capital markets are seen as an important facilitator of the change needed to tackle climate change and encourage sustainability. International and national commitments to reduce greenhouse gases are now beginning to translate to tougher disclosure and reporting requirements for banks and insurers, while growing awareness of social inequalities is leading to new requirements around diversity, pay and supply chains.

"ESG has become one of the biggest issues for financial institutions," says **David Van den Berghe, Global Head of Financial Institutions at AGCS**. *"Financial services may be ahead of many other sectors when it comes to addressing this topic, but it will still be an important factor shaping risk for many years to come. Social and environmental trends, such as diversity and climate change are increasingly sources of regulatory change and liability, while increased disclosure and reporting will make it much easier to hold companies and their boards to account."*

Growing regulatory risk

Up until now, ESG disclosure and reporting has been largely voluntary, driven by growing demand from investors for increased transparency and information on sustainability and climate change. However, a transition towards rules-based and compulsory ESG regimes is underway.

According to law firm, **Herbert Smith Freehills**[1], there have been over 170 ESG regulatory measures globally since 2018, with Europe leading the way, accounting for around 65% of all ESG-related regulation. Though no global, standardized and binding ESG reporting or benchmark instrument exists, 'hard law' measures with punitive sanctions are becoming more common.

Europe is steaming ahead with a wide range of ESG initiatives as it seeks to integrate sustainability into the region's financial policy framework in a bid to mobilize finance for sustainable growth and meet the EU's international commitments on climate change. The EU's Non-Financial Reporting Directive and Sustainable Finance Disclosure Regulation (SFDR) obligates companies to report on a wide variety of ESG-related metrics. Significantly, in June 2020 the European Commission welcomed the adoption by the European Parliament of the Taxonomy regulation – a standard classification system, establishing a list of environmentally-sustainable economic activities.

Ultimately, these changes will influence how, and in which sectors, companies and funds invest, as they consider whether a particular asset fits within the taxonomy or ESG strategy, how they will report about it and what stakeholders and shareholders will think, according to **Hannah Tindal, Regional Head of Directors And Officers, UK, AGCS**.

"ESG regulations and guidance will be a driver of risk going forwards. With new rules on disclosure and taxonomy, and around green investments, the compliance risk for financial institutions is growing," says Tindal.

Outside of Europe, the new Democrat administration of President Joe Biden is expected to signal a shift in ESG policy in the US, with more '**rules-based**' disclosure now on the cards. The Federal Reserve recently joined the global central banks' Network for Greening the Financial System while the Securities Exchange Commission (**SEC**) has launched a review of climate-related disclosure for public companies.

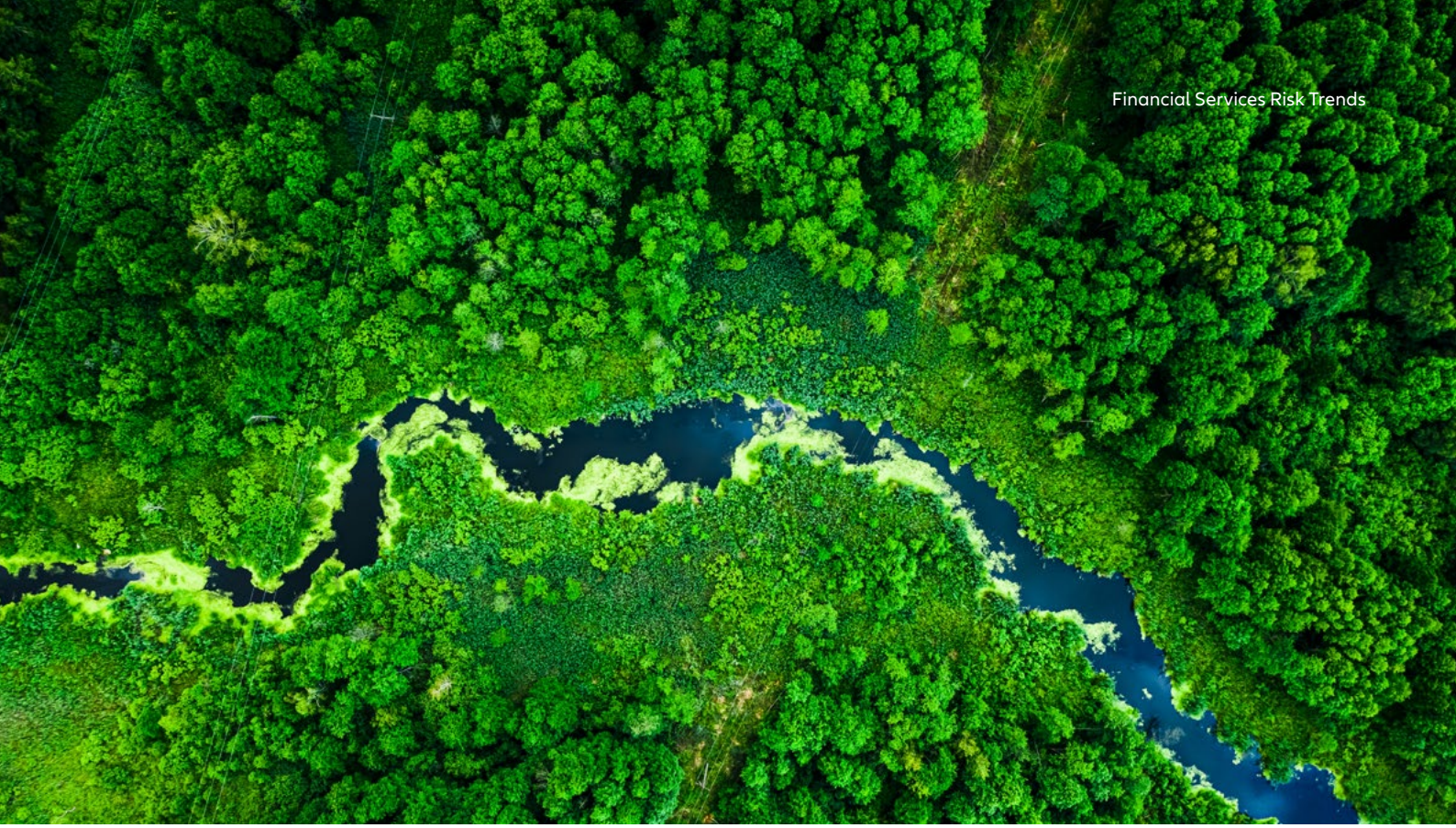
"The new Biden administration is likely to result in a period of regulatory change, including the potential for an ESG framework for financial institutions in the US. Financial institutions should anticipate swift and sudden changes in US regulation around ESG, although these changes may not follow the same approach taken in other markets like Europe," says **Anton Lavrenko, Regional Head of Financial Institutions, North America, at AGCS**.

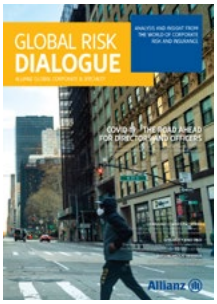
At an international level, global accounting standards setter the International Financial Reporting Standards (IFRS) is consulting on whether to create sustainability reporting standards, while the G20's Financial Stability Board is due to set out plans to build on its Task Force for Climate-related Financial Disclosures (TCFD). The **UK** government said in March 2021 that it intends to make TCFD mandatory for public companies by 2022.

Find out more about ESG topics to watch

ESG moves into the mainstream (and boardroom) | AGCS

1 Herbert Smith Freehills, Spotlight on Malaysia: The Increasing Importance On Effective ESG Risk Management, February 2021





Find out more about diversity and directors and officers litigation and how companies can best manage the changing landscape

Diversity and directors and officers litigation | AGCS

Environmental regulation and litigation

The past decade has seen marked progress on international co-operation and commitments to address climate change and greenhouse gas emissions. Practically every country has signed the Paris Agreement, which calls for keeping the global temperature to 1.5°C above pre-industrial era levels in order to avoid the worst of warming, and a growing number of countries are striving to achieve carbon neutrality within the next two decades.

These commitments are now materializing as government policy and regulation, in a wide range of areas, including climate change reporting and disclosure and greenhouse gas emissions controls. By mid-2019, more than 1,600 laws and policies relating to climate change had been created across 164 jurisdictions, according to law firm **Herbert Smith Freehills**[2]. This surge of climate and sustainability-related regulation, in combination with inconsistent approaches across jurisdictions and a lack of data availability, represents significant operational and compliance challenges for companies.

Climate change is also giving rise to litigation, which is beginning to include financial institutions. These cases have tended to focus on the nature of investments, although more recently there has been an escalation in the use of litigation by activists and advocacy groups seeking to advance climate policies, drive behavioral shifts and force disclosure debate. For example, investors sued Commonwealth Bank of Australia (CBA) in 2017 over a proposed investment in a controversial coal **mine**. The claim was eventually withdrawn when CBA increased its disclosure. Outside of financial services, more recently, non-profit law firm, **ClientEarth**, forced the closure of a giant coal plant in central Poland.

2 Herbert Smith Freehills, 25-Fold Rise In Climate Change Related Regulation Could Mean Businesses Are Facing Risks To Value and Reputation, Says New Report, September 2019

Social changes driving risk

In recent years, the social aspect of ESG has become more prominent, with growing concern for the effects of inequalities and social injustice, made more apparent in the past year by Covid-19 and "Black Lives Matter" protests. Against this backdrop, the broader social responsibilities of business are coming under scrutiny.

Board pay and diversity is a particularly hot topic. Norway's $1trn sovereign fund – one of the world's largest – is just one that has developed active stewardship of management compensation proposals in the companies it invests in, amid concerns about opaque pay. At the same time, a growing number of companies are looking at linking CEO or director level remuneration to climate/ESG-related targets, such as greenhouse gas reduction.

Diversity is rapidly becoming a regulatory issue. The UK's Financial Conduct Authority (FCA) is exploring diversity requirements as part of its listing rules. Over the past year, there has been a big uptick in board diversity litigation, particularly in the US, with cases typically alleging a failure in the fiduciary duties of directors given the inadequate level of diversity on the board or in management positions. A number of studies show diversity brings better risk management and financial performance to a board.

Tackling greenwashing

Banks and insurers are already under increasing pressure from environmental groups to withdraw their support of industries involved with carbon intensive activities, such as new oil, gas and coal projects. More recently, firms are being challenged over their financing for a wider range of environmentally damaging industries, such as beef or soya farming in the Amazon, palm oil in Malaysia and oil exploration in Africa. A number of institutional investors decided not to invest in food delivery service Deliveroo's 2021 IPO in London due to concerns over pay and conditions.

Regulators and pressure groups are increasingly likely to turn the spotlight on greenwashing, in which companies provide misleading information in order to present a more environmentally-friendly and responsible public image. Companies have already been the subject of litigation in the US. In the UK, the FCA has developed a set of principles to tackle concerns over false claims. The Task Force on Climate-Related Financial Disclosures, the SEC in the US and European supervisors are also looking at this issue more closely.

With more compliance, it will be easier for regulators, investors and other stakeholders to hold companies to account on social and environmental issues, says Lavrenko. Pressure groups, for example, often use institutions' own ESG reports to do so when it comes to assessing carbon-neutral targets.

"Companies that commit to addressing climate change, diversity and inclusion will need to follow through," says Lavrenko. *For those companies that do not, it will come back to haunt them."*

Q&A: The ESG landscape

Allianz Global Investors *(AGI) has been incorporating ESG factors into its investment decisions for over 20 years. In this Q&A,* ***Joe Pursley, Director of Insurance, AGI****, highlights some of the key trends it sees in this space for financial institutions.*

What would you consider to be the most important ESG issues for financial institutions?
The most important ESG issue we see today is making sense of ESG data and disclosures. There are a multitude of ESG data providers and data points in the market, and accessing and understanding ESG data is not as straightforward as understanding traditional financial metrics. While the industry has made significant progress, we currently do not have standardized methodology for evaluating or reporting ESG data, nor disclosing ESG information that various stakeholders may find useful. The trend is moving in the right direction globally though, led by the adoption of the EU Taxonomy and the Sustainable Finance Disclosure Regulation (SFDR) in Europe. In the US, some states are now looking at mandating disclosure of certain ESG data points, and the Securities Exchange Commission recently announced that it would be looking into updating climate risk disclosures for public issuers. We are confident ESG standardization will come, but, like anything in finance, it will take time and collaboration, with financial institutions playing a key role.

What can be some of the negative consequences for financial institutions if they don't adequately manage these issues?
Some financial institutions will choose to wait until a clear industry standard methodology (or regulatory requirement) is established. We disagree with this view, and believe it is important to "get out in front of the parade before you get run over by it." By taking a proactive approach to ESG integration today, financial institutions can better position themselves for future standardization and prescriptive regulatory requirements and disclosures. By ignoring ESG data and integration, and, importantly, ESG risk factors, financial institutions could find themselves owners of stranded assets or unintentionally expose themselves to emerging risks that could have been considered with thoughtful ESG integration.

How prominent is awareness and effectiveness of managing ESG issues in the sector overall?
We are seeing a significant increase in the awareness of ESG issues among financial institutions. That being said, the effectiveness of managing ESG issues is a slightly more complicated question. For equity holdings, financial institutions can engage with management and vote their proxies to reflect ESG priorities. Bondholders, on the other hand, do not have the same voting rights and often need to be more creative when engaging with issuers, which can make managing ESG issues less straightforward. Having said that, we strongly believe that asset owners need to be just that – asset owners. We think bondholders in particular hold significant power to create positive ESG change due to the sheer size and scope of capital they control. It is still early days, but bondholders are beginning to better understand the potential power they possess to mandate ESG change, especially when grouping together to make their voices heard. The UN-convened Net-Zero Asset Owner Alliance is an international group of institutional investors who are committed to transitioning their investment portfolios to net-zero greenhouse gas emissions by 2050, and is a great example of how large financial institutions with significant holdings in both equities and fixed income can unite to effect positive ESG change. We believe this trend will continue to grow over the next several years.

In which areas are you seeing the most interest from financial institutions?
We are seeing interest in ESG capabilities from two separate, but complimentary angles. The first area of interest we are seeing is for traditional strategies (e.g. Core Fixed Income and Public Equities), but with a fully integrated ESG approach which incorporates the analysis of various ESG risk factors, and potentially eliminates certain "sensitive sectors" from eligibility within the portfolio from a risk-based perspective. AGI has incorporated ESG factors into our investment decisions for over 20 years, and we believe we are an industry leader in managing "Integrated ESG" portfolios across asset classes, including in both equity and fixed income.

Of particular note in this space would be our ESG Integrated strategies in US/European fixed income, Emerging Market debt and Global equities. The second area of interest we are seeing is more focused on ESG "Impact" strategies, where financial institutions have the ability to quantify measurable and attributable change created through their investments. These allocations are typically much smaller than "Integrated ESG" strategy allocations, but their importance is significant, as the majority of a financial institution's ESG reporting metrics within their investment portfolio are derived from "Impact" investments. Because of this, we are seeing significant interest in strategies like Green Bonds, Social Bonds, Renewable Energy Infrastructure (equity and debt) and, most recently, strategies that focus on producing a measurable positive social impact within society. We believe financial institutions' focus on "Impact" investments will only grow as an increasing number of firms begin to produce sustainability reports and measure how their investments are creating positive change.

Growing emphasis on risk management

As investment decisions are increasingly influenced by this new environment, so too will be the role of risk management and in particular that of the board of directors. Questions and clarity about who is responsible for ESG topics, such as climate change, on the company board will not just be a matter of "nice to have" but essential if the duties of directors are considered to be adequately fulfilled in future.

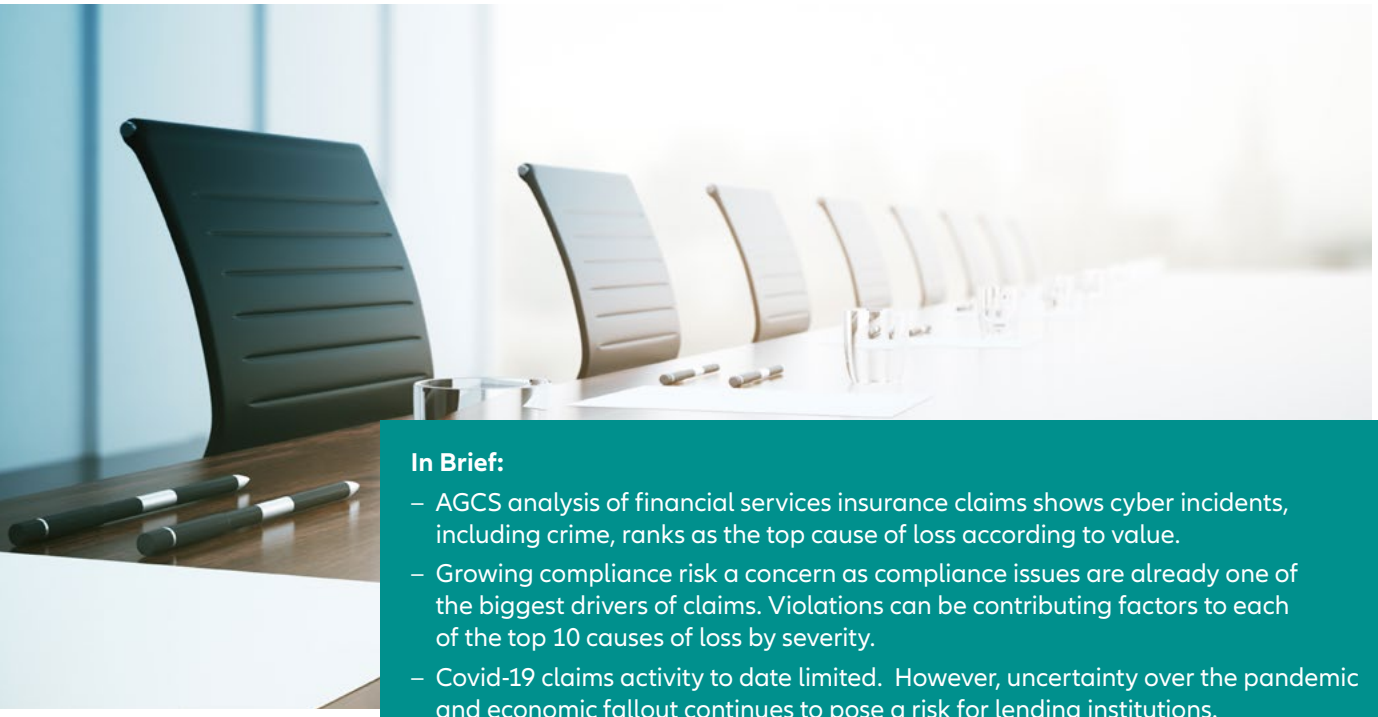
ESG was named by 38% of financial institutions as being one of the three risk types that will increase the most in importance over the next two years, more than for any other, according to a recent Deloitte **global risk management survey**[3]. However, only a third of respondents considered their institutions to be extremely or very effective at managing ESG risk.

It is important that ESG is not only on the board agenda a few times per year but that a company embeds sustainability topics and thinking into the whole organization. Beyond internal steering, it is also crucial for the board to acquire appropriate skills and understand the external requirements in order to be successful in the long-term. Financial institutions will also need to monitor carefully how expectations regarding ESG evolve among regulators, investors, and customers.

"Elevating and identifying ESG risks through a business' risk registers and committees and making sure it is understood how they will perform in and out of the boardroom, is crucial," says **Shanil Williams, Global Head of Financial Lines at AGCS**. *"Disclosure is not just about the various regimes coming in around the world but also about how you disclose to the wider community – employees, stakeholders and the media – the latter, in particular, can have a devastating impact on reputation.*

"We are already utilizing ESG data in our D&O insurance underwriting," adds Williams (as part of a partnership with investment and risk consultant, ***the Value Group****). "We have statistically modeled ESG data points against claims and public litigation and we do see some predictive power there. From an insurer's point of view, conversations around ESG-related topics, in addition to financial topics, are becoming much more important."*

3 Deloitte Insights, Global risk management survey 12th edition



In Brief:

- AGCS analysis of financial services insurance claims shows cyber incidents, including crime, ranks as the top cause of loss according to value.
- Growing compliance risk a concern as compliance issues are already one of the biggest drivers of claims. Violations can be contributing factors to each of the top 10 causes of loss by severity.
- Covid-19 claims activity to date limited. However, uncertainty over the pandemic and economic fallout continues to pose a risk for lending institutions.

5 The claims picture

Compliance issues are one of the biggest drivers of insurance claims involving financial institutions, although losses related to the sector's growing reliance on technology are also on the rise.

Insurers continue to see large claims among financial institutions relating to compliance and increased regulatory activity. Despite operating in Covid-19 conditions, the US **Securities and Exchange Commission**[1] (SEC) collected a record $4.7bn in fines in fiscal 2020 across 715 separate cases, including foreign bribery charges, disclosure and accounting violations and misconduct.

The compliance burden for financial institutions has increased significantly over the past decade in particular. Regulatory enforcement has intensified as banks and senior management are more readily held to account by regulators and prosecutors, as well as shareholders. At the same time, they are subject to a growing bank of rules and regulations in a diverse range of areas, including sanctions, whistle blowing, data protection and cyber security laws, as well as a host of environmental, social, and governance (ESG) requirements.

"Compliance issues are one of the biggest drivers of insurance claims for financial institutions," says **David Ackerman, Global Claims, Key Case Management at AGCS**. *"They operate in challenging times, with technological changes and shifting political and regulatory developments. Keeping abreast of compliance in a rapidly-changing world is a tough task for companies and their directors and officers."*

"Compliance challenges have been an ongoing issue for financial institutions since the global financial crisis of 2008," adds **Shanil Williams, Global Head of Financial Lines at AGCS**. *"Their compliance burden is enormous, and is now accompanied by growing regulatory activism, legal action and litigation funding."*

1 US Securities And Exchange Commission, 2020 Annual Report, Division of Enforcement

Claims analysis

Top 10 causes of loss by value

Computer System/Network Security Error, Violation or Breach or Crime	12%
Negligence	11%
Company/Insured v Insured (e.g. board v board)*	6%
Employee Dishonesty	5%
Shareholder Derivative Action	5%
Fraud/Embezzlement/Intentional Misconduct	5%
Government Claim or Investigation	4%
M&A Warranty Breach (e.g. seller/buyer merger and acquisition dispute)	4%
Breach of Trust or Duty	4%
Mis-selling	4%

Based on the analysis of 7,654 claims worth approximately €870mn ($1.05bn) reported from January 1, 2015 to March 31, 2021. Total includes the share of other insurers involved in the claim in addition to AGCS. Percentage shares are rounded up or down accordingly. Graphic shows breakdown of top 10 causes of loss only. Other causes of losses were also identified in the data analysis.

*Driven by historical loss experience

Source: Allianz Global Corporate & Specialty

Top 5 causes of loss by value by selected policies

Directors and Officers

1	Company/Insured v Insured*	22%
2	Shareholder Derivative Action	19%
3	Securities Violations/ Shareholders Disputes (direct)	7%
4	Class Action (customers)	7%
5	Governmental Claim or Investigation	7%

Based on the analysis of 3,349 claims worth approximately €225.7mn reported from January 1, 2015 to March 31, 2021. Total includes the share of other insurers involved in the claim in addition to AGCS. Percentage shares are rounded up or down accordingly.

Crime

1	Employee Dishonesty	41%
2	Fraud/Embezzlement/ Intentional Misconduct	18%
3	Non-Compliance with Laws and Regulations	9%
4	Computer System or Network Security Error, Violation or Breach or Crime	6%
5	ATM Loss	3%

Based on the analysis of 894 claims worth approximately €106.4mn reported from January 1, 2015 to March 31, 2021. Total includes the share of other insurers involved in the claim in addition to AGCS. Percentage shares are rounded up or down accordingly.

Professional indemnity

1	Negligence	19%
2	Computer System/Network Security Error, Violation or Breach or Crime	16%
3	Mis-selling	7%
4	Breach of Trust or Duty	7%
5	Fraud/Embezzlement/ Intentional Misconduct	5%

Based on the analysis of 2,921 claims worth approximately €485.4mn reported from January 1, 2015 to March 31, 2021. Total includes the share of other insurers involved in the claim in addition to AGCS. Percentage shares are rounded up or down accordingly.

* driven by historical loss experience

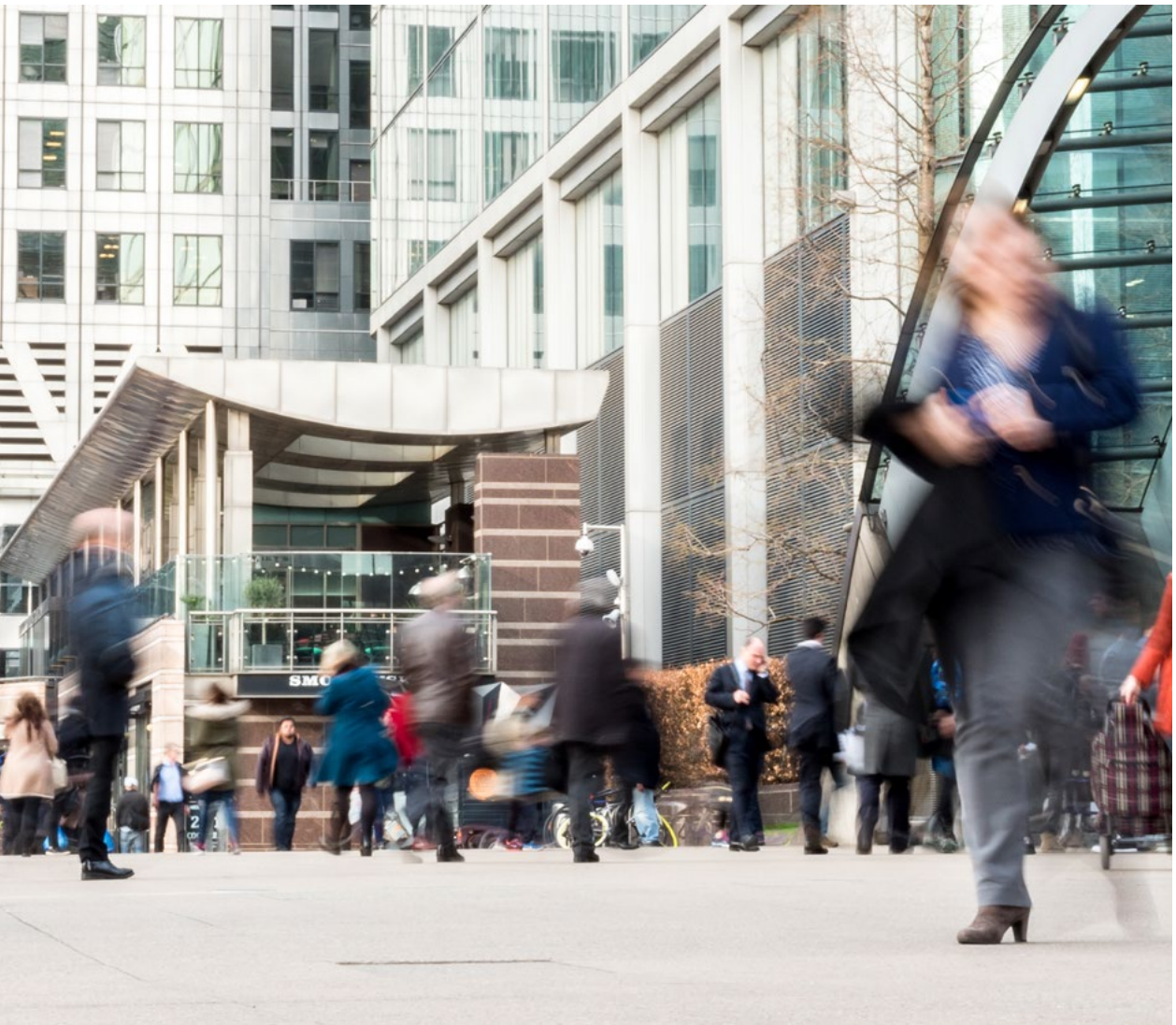
Source: Allianz Global Corporate & Specialty. Graphics show breakdown of top five causes of loss only. Other causes of losses were identified in the data analysis.

Complexity a major factor

Claims against directors and officers arising out of underlying prosecutions of banks have become a significant severity driver, explains Ackerman. In particular, the insurance market has seen a number of very large claims against directors and officers that have arisen out of investigations and prosecutions for sanctions breaches in the US. Enforcement of the Foreign Corrupt Practices Act (FCPA) continues to be a high priority area for the **SEC**, which last year agreed to a $3bn settlement with Goldman Sachs in connection with **Malaysia Development Berhad bribery charges**.

Mergers and acquisitions and initial public offerings have also generated large claims in recent years, as have money laundering, tax and accounting fraud, currency cartels and collusion, and large insolvencies. In 2019, the European **Commission** fined five banks (Barclays, RBS, Citigroup, JPMorgan and MUFG) €1.07bn for operating cartels in the foreign exchange markets – the banks also faced a **$1bn** class action in the UK linked to the scandal.

Typically, large compliance claims are long tail – they can last upwards of 10 years – and involve complex regulatory investigations, prosecutions, large fines or settlements, and potentially shareholder derivative actions, says Ackerman.



Concerning developments

Securities class actions are being filed in record numbers, rising steadily over the past 10 years. There were a record 268 US class action filings in 2019, although this fell to 210 in 2020, with financial institutions among the top three most targeted sectors, according to law firm **Woodruff Sawyer**[2]. However, this still exceeded the 10-year average by 13%. Shareholder class actions have also been on the rise in the **UK**, Canada and Australia (according to a report by broker **Marsh**[3] in 2018, the average number of securities class action claims lodged per year in Australia increased four-fold in 10 years), and to a lesser extent **Europe**.

Increasing frequency and severity of derivative actions against directors and officers of financial institutions and consumer/customer class action claims is also concerning, according to Ackerman.

"We are seeing more claims made against directors on behalf of the institution, looking to recover damages due to the failure of directors and officers to exercise their duty, for example, in areas like sanctions. In addition, derivative actions by shareholders following a regulatory investigation did not historically result in large losses, but this is no longer the case. In a number of countries – including Australia and Israel – we have seen large claims from derivative actions," says Ackerman.

2 Woodruff Sawyer, 2020 Securities Class Actions Exceed the 10-Year Average, January 2021
3 Marsh, Shareholder class actions shaping the future of Australia's D&O insurance landscape, August 2018

Early days for Covid claims

AGCS has received claims notifications related to Covid-19 in the US and elsewhere, although, at the time of writing, the pandemic has not yet given rise to large numbers of financial lines insurance claims overall, in part due to government support and stimulus packages, and the dramatic recovery of stock markets in 2020.

To date, any claims against financial institutions related to the pandemic have emerged in only a few distinct areas: non-payment of business interruption claims by insurers and claims against banks relating to their administration of loans under the US Cares Act Paycheck Protection Program (PPP). A smaller number of claims have also been made by investors against asset managers alleging they failed to disclose risks associated with the pandemic or reacted adequately to Covid-19 risks.

However, uncertainty over the pandemic and economic fallout continues to pose a risk for lending institutions, says **David Ackerman, Global Claims, Key Case Management at AGCS**.

Economic downturns and insolvency are typically a driver for financial institutions claims, as shareholders, customers and insolvency practitioners seek to recoup losses. Insolvency related claims against directors and officers and under professional indemnity insurance are expected, although government support during the pandemic has softened the impact of Covid-19 and kept the number of insolvencies down to date, Ackerman explains.

"Covid-19 is the systemic loss event of the moment. We have had claims notifications, but the pandemic has yet to generate losses of consequence. However, we are not out of the woods yet, and it is not clear how deep or broad the economic downturn is," says Ackerman. *"Insolvency claims have yet to materialize, as was first anticipated, but they may yet do so as government support for the economy and business is unwound.*

"If there were substantial amounts of unsecured debt on banks' balance sheets, we could see shareholder class actions and regulatory activity if financial institutions were themselves to struggle. Potentially, we could also see claims against investment managers where they have failed to advise investors and where customers suffered losses to their portfolios."

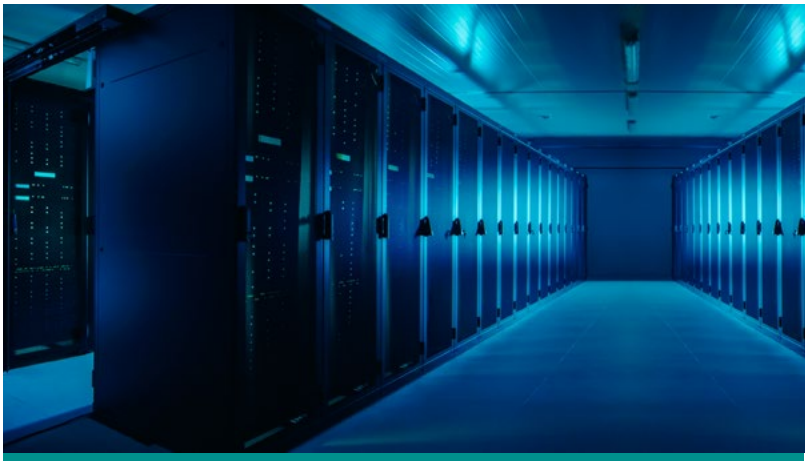
Mis-selling and systemic issues

Mis-selling is another big driver of claims in recent years. A number of countries have experienced scandals related to financial services, such as insurance, investment products and loans.

"There is severity of claims for mis-selling in insurance and investment management, where firms have been accused of not providing appropriate advice, or wrongly charging for products," says Ackerman. *"The insurance industry saw a large number of claims notifications in Australia following the findings of the* ***Royal Commission into Misconduct in the Banking, Superannuation And Financial Services Industry*** *but this is not a problem that is unique to Australia,"* says Ackerman.

Systemic or aggregate claims remain the biggest cause of loss. Events such as a financial crisis or the Covid-19 pandemic or market-wide compliance or conduct issues can lead to losses across companies, geographies and lines of insurance business.

"There have been a number of systemic events to hit the financial institutions sector that have caused significant insurance losses, such as claims against directors and officers for compliance breaches at banks or claims that have arisen from sanctions breaches," says Ackerman.



Tomorrow's claims – the rise of technology-related losses

AGCS is also seeing a growing number of insurance claims linked to the sector's reliance on technology, such as claims arising from electronic exchanges, data breaches and cyber crime.

"The world is changing rapidly with the growing use of data and technology," says **David Ackerman, Global Claims, Key Case Management at AGCS**. *"One area in which we have seen an increase in the frequency of claims is through the use of technology by criminals to steal money or commit fraud. We are also seeing increasing regulation around technology, and data protection and privacy in particular. Insurers have already seen a number of claims made against directors following major privacy breaches,"* says Ackerman.

In particular, AGCS has seen a number of sizable claims related to fraudulent payment instructions and "fake president" scams. Often, these claims will involve a degree of human error or compliance failings on the part of bank employees, such as the failure to properly evaluate whether a payment is valid, explains Ackerman.

"In one recent claim, the policyholder satisfied a payment instruction, unaware that criminals had monitored its electronic communications, before sending a fraudulent payment instruction. Unfortunately, the bank's employee made the transfer without making the call to validate that the payment request was legitimate." The payment was in the *"several millions of dollars"*.

AGCS has also handled a number of liability claims arising from technical glitches with exchanges and electronic processing systems.

"We have seen claims where systems have gone down and clients have not been able to execute trades, and have made claims against policyholders for loss of opportunity. We have also had claims where a system's failure has caused damages to a third party," says Ackerman. *"In one claim, a fault in an electronic system caused significant currency valuation losses for users. In another incident, one financial institution suffered a significant loss after an electronic trading system crashed following a major revamp, causing processing failures for customers."*

In Brief:

- Loss activity and Covid-19 uncertainty have contributed to a recasting of the insurance market characterized by adjusted pricing and an enhanced focus on risk selection by insurers.
- A growing number of companies are partnering with insurers on alternative risk transfer solutions to manage risk and regulatory capital requirements.

6 Market dynamics – insurance outlook

After more than a decade of falling premium rates, the financial institutions insurance market has undergone a correction over the past year to adjust for higher exposures and claims, particularly for directors and officers.

According to **Marsh's**[1] quarterly Global Insurance Market Index, pricing in financial and professional lines had the highest rate of increase across the major insurance product categories in the fourth quarter of 2020. Financial and professional lines insurance rates increased 47% with increases of 28% in the US, 22% in Europe and 90% in the UK.

"The financial institutions insurance market is adjusting to more than a decade of increased exposure and losses since the global financial crisis in 2008, as well as a broader hardening of the commercial and specialty insurance market, says **Shanil Williams, Global Head of Financial Lines at AGCS**. *In addition, insurers are conscious of potential claims arising from the pandemic and uncertainty around the economic consequences."*

"The insurance market for financial institutions risks is likely to remain firm in 2021, supported by ongoing uncertainty around Covid-19," says Williams. *"Rates have been increasing and many insurance carriers have restricted capacity in some areas where exposures are highest."*

1 Marsh, Global Insurance Index 2020 Q4

Interest in alternative risk transfer continues to grow

Insurance is increasingly an important part of the capital stack of financial Institutions who are looking more and more at alternative risk transfer (ART) and financing strategies, in addition to traditional insurance coverages.

A growing number of companies are partnering with insurers to manage risk and regulatory capital requirements in an optimized fashion or to the unlock the value of collateral, exploring a range of bespoke solutions *(see examples below)* that can help companies to achieve the right balance of return, risk and capital for their businesses.

"Providing capital relief to banks on their loan and credit line portfolios is an area of growing interest," says **Grant Maxwell, Global Head of ART at AGCS**. *"ART solutions can help with liquidity facilities for securitization of unusual asset portfolios or wrapping of collateral for lending opportunities where the collateral is difficult for the lender to recognize or analyze."*

In addition, risk transfer solutions can also be utilized for improving company valuation, an interesting consideration for private equity firms, for example.

With some budgets under pressure in a harder insurance market, financial institutions are also increasingly exploring ways to make use of captive insurers to compensate for changes in the insurance markets or finance more difficult to place risks.

"An increasing number of clients in the financial institutions space are inquiring about captives and alternative risk transfer solutions to manage elements of their directors and officers (D&O), cyber and error and omissions (E&O) programmes, for example," says **Christof Bentele, Head of Client Management for ART at AGCS**. *"But also beyond financial lines insurance products, we are seeing a growing interest in structured insurance or reinsurance solutions, spanning across a variety of risks and insurance classes of business. Clearly, this goes along with an increased appetite for risk retention by financial institutions."*

Each transaction typically is situation-specific, reflects the company's objectives and limitations and is consequently individually structured, analyzed and modeled.

Covid-19 crystalization

Covid-19 has crystalized an already hardening insurance market. The property/casualty market as a whole has paid out large losses from natural catastrophes in recent years, while social inflation trends in the US have impacted casualty lines. Many insurers have reviewed risk appetites over the past 12 months and in many cases withdrawn or scaled back their participation in unprofitable or high exposure lines of business. Financial institutions insurance has not been immune to this trend.

For **financial lines** underwriters have one eye on an unprofitable past and the other on an uncertain looking future. Although varying by class and geography, the financial institutions market has seen significant withdrawals of capacity, although recent months have also seen some new participants enter the market. Although coverage remains broad, insurers have sought to clarify areas of uncertainty in certain markets, most notably around the pandemic and cyber risks.

Insurers have been particularly cautious in lines that have seen large losses or that have significant exposure to Covid-19, in particular professional indemnity and directors and officers, which have seen some of the largest price adjustments and pressure on capacity, retentions and limits. According to Marsh, D&O rates for US publicly traded companies increased 44% in the fourth quarter of 2020, with even bigger increases in the UK. Commercial crime rates increased 80%.

Examples of ART deals

1: A US-based life insurance company had to set up reserves for its portfolio of individual fixed annuities. The reserves mandated by the regulators were based on unreasonable assumptions, and were in excess of the economic reserves. The difference between the regulatory reserves and excess reserves was financed by a bank by issuing a contingent letter of credit. As the annuity portfolio grew, the size of the letter of credit exceeded the bank's exposure limit. ART co-participated on the letter of credit, which reduced the bank's net exposure and allowed it to continue to expand the business.

2: The company is in the business of providing a liquidity facility agreement ("LFA") for securitizations. Under the Basel III rules, the capital treatment of the LFA follows that of the most senior note in its corresponding securitization, somewhat regardless of the particular features of the LFA and indeed the securitization. Owing to ART's ability to recognize the very strong overcollateralization of the LFA, ART was able to provide the client with regulatory compliant paper which allowed it to treat the LFA as AA-rated, thereby materially improving the capital treatment of the underlying business.

3: A portfolio of green energy loans had been securitized, with a rating agency mandated interest reserve facility. The reserve facility was trapping some of the cash that could be used to extend new loans. ART provided a non-cash liquidity facility utilizing its high credit rating. The facility allowed the sponsor to free up the needed working capital.

Further information

Global Industry Solutions: **Financial Services**

The world's largest retail and universal banks, (re)insurance companies, asset managers, venture capital/private equity funds, financial advisors and intermediaries, just to name a few, trust AGCS' expertise to navigate critical changes in the financial landscape. They are confident in our ability to manage risks, resolve unique financial services challenges and to innovate.

Our reputation as leaders of the most complex global risks in the financial services industry has been earned by maintaining a close, consistent dialogue with our clients. This reputation is backed by significant underwriting capacity to cover the largest exposures and is underpinned by the strongest Standard & Poor's rating of any global property and casualty insurer

We field a dedicated Financial Services Global Industry Solutions team with a comprehensive product range and a network across more than 200 countries.

Solutions:

Holistic approach – our team of specialists craft a variety of products for banks, asset managers, insurance and private equity to transfer risk.

Strong client relationships – client-centric deal and servicing teams deliver sustainable solutions across geographies and risk.

Alternative Risk Transfer – tailor-made solutions, particularly useful when unique challenges arise, can be customized to the smallest detail without using traditional business insurance.

Underwriting teams with thorough financial industry expertise, identify and develop solutions for each specific challenge.

Global claims experts lead complex claims through a dedicated "single point of accountability" manager.

Our experienced risk consultant engineers from a wide range of technical and scientific disciplines provide in-depth analysis.

Centrally coordinated global insurance programs respond to cross-border exposures and regulatory/ fiscal frameworks.

AGCS has established the gateway role of Industry Solutions Director for Financial Services to develop advanced solutions for our financial services customers. Find out more about our solutions at

Financial Services insurance | Allianz

Contacts

Martin Zschech
Global Head of Industry Solutions
& Client Management
Global Industry Solutions Director
for Financial Services
martin.zschech@allianz.com

Shanil Williams
Global Head of Financial Lines, AGCS
shanil.williams@allianz.com

Anton Lavrenko
Head of Financial Institutions,
North America, AGCS
anton.lavrenko@agcs.allianz.com

Marek Stanislawski
Global Cyber Underwriting Lead, AGCS
marek.stanislawski1@allianz.com

David Ackerman
Global Claims Key Case Management, AGCS
david.ackerman@allianz.it

Christof Bentele
Head of Client Management for
Alternative Risk Transfer, AGCS
christof.bentele@art-allianz.com

Jeremy Sharpe
Global Head of Distribution, AGCS
jeremy.sharpe@allianz.com

David Van den Berghe
Global Head of Financial Institutions, AGCS
david.vandenberghe@allianz.com

Hannah Tindal
Head of Directors And Officers, UK, AGCS
hannah.tindal@allianz.com

Thomas Kang
Head of Cyber, Tech and Media,
North America, AGCS
thomas.kang@agcs.allianz.com

Grant Maxwell
Global Head of Alternative Risk Transfer, AGCS
grant.maxwell@art-allianz.com

Contacts

For more information contact your local Allianz Global Corporate & Specialty Communications team.

Asia Pacific
Wendy Koh
wendy.koh@allianz.com
+65 6395 3796

Mediterranean/Africa
Florence Claret
florence.claret@allianz.com
+33 158 858863

Lesiba Sethoga
lesiba.sethoga@allianz.com
+27 11 214 7948

Global
Hugo Kidston
hugo.kidston@allianz.com
+44 203 451 3891

Heidi Polke-Markmann
heidi.polke@allianz.com
+49 89 3800 14303

Central and Eastern Europe
Daniel Aschoff
daniel.aschoff@allianz.com
+49 89 3800 18900

North America
Sabrina Glavan
sabrina.glavan@agcs.allianz.com
+1 646 472 1510

Ibero/LatAm
Camila Corsini
camila.corsini@allianz.com
+55 11 3527 0235

UK, Middle East, Nordics
Ailsa Sayers
ailsa.sayers@allianz.com
+44 20 3451 3391

For more information contact **agcs.communication@allianz.com**

Follow Allianz Global Corporate & Specialty on

Twitter **@AGCS_Insurance #fsrisktrends** and

LinkedIn

www.agcs.allianz.com

Disclaimer & Copyright

Copyright © 2023 Allianz Global Corporate & Specialty SE. All rights reserved.

The material contained in this publication is designed to provide general information only. Whilst every effort has been made to ensure that the information provided is accurate, this information is provided without any representation or warranty of any kind about its accuracy and Allianz Global Corporate & Specialty SE cannot be held responsible for any mistakes or omissions.

Allianz Global Corporate & Specialty SE
Dieselstr. 8, 85774 Unterfoehring, Munich, Germany

Images: Adobe Stock/iStockPhoto

All currencies US$ unless specified

January 2023