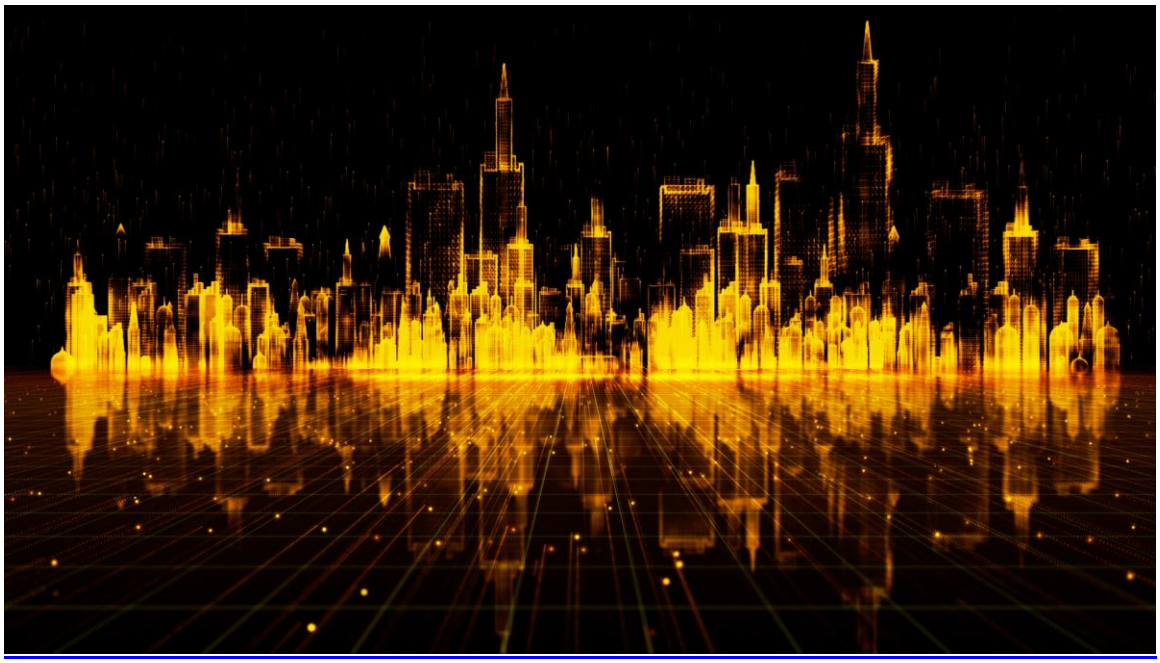
Basel iii Compliance Professionals Association (BiiiCPA)
1200 G Street NW Suite 800 Washington DC 20005-6705 USA
Tel: 202-449-9750 Web: www.basel-iii-association.com



Basel iii News, February 2023

Dear members and friends,

We have some interesting BIS international banking statistics and global liquidity indicators.

• Banks' cross-border claims, which comprise mainly loans, debt securities and derivatives with a positive market value, increased by *$1.1 trillion* in Q3 2022, raising the year-on-year growth rate to 10%. Derivatives drove this increase.

• Of this total, the change in cross-border credit, defined as loans and holdings of debt securities, was only $169 billion. Euro-denominated credit outpaced dollar credit, which remained virtually unchanged.

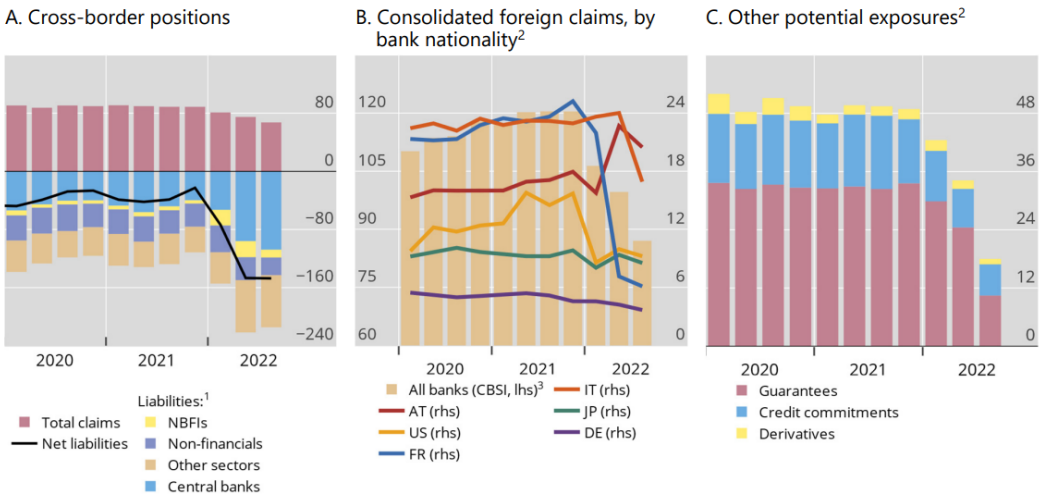
• Credit to advanced economies continued to grow, while that to emerging market and developing economies1 fell, driven by a contraction in credit to China and Hong Kong SAR. Foreign claims on Russia fell by a third since end-2021.

• In the BIS global liquidity indicators, dollar credit to non-banks in EMDEs fell sharply, whereas credit in euro and yen expanded. The contraction in dollar credit mainly reflected a drop in bank loans.

• The stock of international debt securities denominated in US dollars issued by EMDEs declined for the first time since the Great Financial Crisis of 2008–09.

Bank exposures to Russia

Outstanding amounts, in billions of US dollars — Graph 4



Panel A covers all BIS reporting banks, including banks in China and Chinese banks in other reporting countries. Panels B and C exclude Chinese banks, as Chinese authorities do not report the CBS.

[1] Liabilities (by counterparty sector) are shown as negative figures on the vertical scale. [2] Consolidated, on a guarantor basis (CBS/G). [3] On an immediate counterparty basis (CBS/I). Partial data from the BIS locational banking statistics suggest that Chinese banks increased their claims on Russia in 2022, accounting for over a third of all cross-border claims on Russia at end-Q3 2022.

Source: BIS consolidated and locational banking statistics.

Banks' exposures to Russia continued to fall

Banks continued to reduce their cross-border claims on Russia in Q3 2022, even as their liabilities to the country remained elevated (Graph 4 below).

Cross-border claims to Russia dropped by $7 billion, the third consecutive quarterly decline (Graph 4.A).

Liabilities to non-bank financial intermediaries (NBFIs) and non-financials in Russia fell by $11 billion and $7 billion, respectively.

At the same time, cross-border liabilities to the Central Bank of the Russian Federation grew by $12 billion in Q3 2022, as blocked coupon payments and redemptions continued to accumulate at Euroclear.

The CBS provide a more comprehensive view of how banks' consolidated exposures to Russia receded in the course of 2022 (Graph 4.B). Since Q4 2021, foreign claims reported on Russia dropped by 28% to $87 billion at end Q3 2022.

Other potential exposures fell by even more (–63%) to reach $18 billion over the same period (Graph 4.C).

French (–$19 billion), US (–$6 billion) and Italian banks (–$6 billion) cut foreign claims the most since end-2021.

To read more: https://www.bis.org/statistics/rppb2301.pdf

Getting the full picture - the road ahead for climate stress testing

Dr Sabine Mauderer, Member of the Executive Board of the Deutsche Bundesbank, at the 2023 European Banking Authority workshop on climate risk stress testing.

1. Introduction

Ladies and gentlemen,

- How does climate change affect the economy?
- What impact does climate change have on growth and inflation?
- How does climate change affect the financial system?

Policymakers need answers to these questions.

Understanding climate-related risks and their transmission channels is essential for designing targeted policies. Central banks and supervisors have outstanding analytical capabilities.

Dealing with financial risks is our bread and butter business. This ample expertise can help to strengthen the understanding of climate-related financial risks. These risks are not a new risk category per se. Climate risk drivers can exacerbate "traditional" financial risks and existing vulnerabilities, such as credit risks and market risks.

Stress tests have been an integral part of the toolbox of central banks and supervisors for a long time. Stress tests provide valuable insights into the risk exposure and resilience of individual banks and the financial system. Climate stress tests can complement common stress tests to give a fuller picture.

2. Climate scenarios – A glimpse of possible futures

Stress tests are forward-looking analytical exercises that build on baseline and adverse scenarios.

The same goes for climate stress tests. This is where climate scenarios come into play. Climate scenarios give us a glimpse of different possible future outcomes. They can help us to understand how climate-related risks could evolve and what the implications might be for the economy and the financial system.

The Network for Greening the Financial System (NGFS) has developed and repeatedly refined a set of six climate scenarios. The scenarios fall into three categories and explore the impact of climate change (physical risk) and climate policy (transition risk). In the orderly scenarios, the early and gradual introduction of climate policies leads to subdued physical and transition risks.

The disorderly scenarios assume that climate policies are delayed or divergent across countries and sectors. These scenarios are associated with higher transition risk as, for instance, carbon prices might need to rise sharply and abruptly.

In the hot house world scenarios, global warming cannot be limited due to insufficient global efforts. As a result, extreme weather events become more severe and more frequent. Physical risks increase drastically.

All these NGFS scenarios help quantify the economic impacts of different emission and policy pathways. They show that both climate change and policies to contain it come at a price. But taking ambitious climate action too late or failing to act altogether would be much more costly in the end.

For instance, what happens if we keep delaying action today but still want to reach net zero by mid-century? This scenario shows that a delayed transition would lead to a drastic surge in carbon prices from 2030 onwards.

By 2050, carbon prices would have to rise to nearly 400 dollars per ton in this scenario. The scenarios already put a price tag on policy action – or lack thereof. In order to further improve the usability of the scenarios, the NGFS is continuously bringing them up to date.

In September 2022, the NGFS published the Phase III update, which introduced several enhancements. For instance, the modelling of physical risks was improved.

This iteration considered, for the first time, the impacts of acute physical risks under different scenarios. In addition, the granularity in the transport and industry sectors was improved, giving a clearer picture of transition risks.

The NGFS scenarios help central banks and supervisors to beef up macro models and climate stress tests.
For example, ECB Banking Supervision used macro-financial scenarios that are based on the NGFS scenarios for its 2022 climate stress test. The Bundesbank is working on a top-down climate stress test that will also build on the NGFS scenarios.

In its 2021 Financial Stability Review, the Bundesbank explored the impact of transition risks on the German financial system. This assessment was also based on the NGFS scenarios.

3. Challenges & way forward

These examples all show that climate scenarios are a useful tool for assessing climate-related risks. Having said that, some obstacles and challenges remain.

Allow me to touch upon three of them.

The first challenge concerns time horizons. Standard stress tests usually look at time horizons of one to three years.

By contrast, climate scenarios have considered much longer time horizons of 10-30 years, as it may take longer for climate-related risks to materialise and for climate policies to have an effect. These long time horizons carry the risk of climate scenarios underestimating the near-term impact of climate-related risk. A number of factors compound the problem.

Which brings me to the second challenge. The non-linearity of climate change means that various tipping points may cause rapid shifts with far-reaching consequences. As a result, climate-related risks are surrounded by deep uncertainty and tail risks cannot be ruled out. For these reasons, the NGFS has described the first climate scenario analyses as learning opportunities that need further fine-tuning.

The NGFS is exploring additional scenarios and looking at options for introducing short-term scenarios. Moreover, the NGFS aims to further expand and improve the sectoral granularity and the geographic coverage as well.

Other factors to consider going forward are geopolitical shifts and changes in global energy markets. Russia's invasion of Ukraine has upended energy markets, with likely long-term impacts for energy prices and energy security.

These developments also carry implications for the transition to net zero and the associated risks. On the one hand, high and volatile prices reinforce incentives to speed up the energy transition and boost renewable energy.

On the other hand, as governments are moving to secure energy supplies and keep energy prices in check, there is a non-negligible risk of carbon lock-in.

For instance, according to the International Energy Agency (IEA), global coal consumption hit an all-time high in 2022.

Likewise, new, longer-term contracts for liquefied natural gas deliveries may complicate the transition away from fossil fuels. In this environment, the NGFS sees a higher risk of a delayed or disorderly transition.

The network is working on including these developments in the upcoming iteration of the climate scenarios. These planned updates will further enhance the usability of the NGFS scenarios.

Last but not least, the issue of data availability and data quality has been a longstanding problem. We all know that the lack of consistent and granular data continues to be an obstacle that complicates the adequate calibration of shocks in stress testing models. Central banks and supervisors can play a part in overcoming this obstacle.

Last summer, the NGFS launched a directory for climate data with over 700 links to relevant data sources. The directory supports financial sector stakeholders in finding relevant climate-related data sources and facilitates access to these data.

In addition, in December 2021, the NGFS published a guide on climate-related disclosures for central banks. The Eurosystem took up this "invitation". Starting in March 2023, it will publish climate-related information on its corporate bond holdings and its non-monetary policy portfolios on a yearly basis.

The Bundesbank already took a first step in July 2022. We published our first climate report and disclosed the climate impact of our non-monetary policy portfolio.

In this way, central banks and supervisors can help to improve the data situation.

Brussels is also taking action to tackle this issue. The EU's Corporate Sustainability Reporting Directive (CSRD) will gradually come into effect from 2024 onwards. The CSRD will require around 50,000 companies to disclose detailed information on sustainability matters.

The initiative will address data gaps, which will also help to increase the reliability of climate stress tests. At the same time, the absence of granular data is no excuse for inaction.

4. Conclusion

Let me conclude.

Climate scenarios and climate stress tests are not perfect yet and the results they provide have to be taken with a grain of salt. Nonetheless, they are already viable instruments for shedding light on the exposure and resilience of banks to climate-related risks.

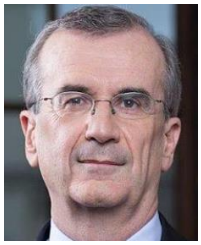
Central banks and supervisors have to continue along this path and further refine climate scenarios and climate stress tests. This includes striking a balance between short-term and long-term scenarios as well as bridging data gaps.

As the work continues, climate scenarios will become more usable and climate stress tests will paint a clearer picture. In order to facilitate progress with climate scenarios and climate stress tests, international coordination and exchange is vital. This workshop is an excellent opportunity to find common ground on the challenges that lie ahead.

To read more:
https://www.bundesbank.de/en/press/speeches/getting-the-full-picture-the-road-ahead-for-climate-stress-testing-738186

Big techs in finance - a bildungsroman that is far from over

François Villeroy de Galhau, Governor of the Bank of France, at the high-level BIS conference "Big techs in finance – implications for public policy", Basel.



Ladies and Gentlemen,

It is a pleasure for me to introduce the second day of this BIS high-level conference on big techs in finance. While it is a pity to do so from a distance, perhaps that is fitting for a conference on the changes in our working lives brought by digital innovation.

Very early on, big techs saw finance as a natural complement – and booster – to their core businesses, launching a technological revolution that might bring many benefits to consumers, across different fields such as payments and stablecoin issuance.

Big techs have met with success on some of these roads, and less so on others. Interestingly, some of these developments do not exactly match what we could have expected even four years ago.

We can therefore consider big techs' entry into finance as a bildungsroman – a sort of coming of age story – with promising early years and somewhat disappointing learning years partly behind us.

Building on this already significant experience, the maturity years may be ahead of us – but that will only be possible under consistent conditions.

I. Big techs and finance: a bildungsroman unfolding under our eyes

A. Promising early years

From the onset big techs were "data rich" and benefited from a global customer base and strong brand recognition.

In order to keep their lead in innovation, big techs acquired a large number of start-ups and fin techs. In the end, their huge financial means enabled them to set up, and then consolidate, powerful oligopolies.
In the wake of US GAFAMs, Chinese BATX emerged to serve their domestic market, and expanded into Asia.

All big techs started diversifying their activities, among others in the financial sector where they first launched innovative digital means of payments, for instance Google Pay in 2011 and Apple Pay in 2014.

This chapter of the book is crystal-clear: big techs were highly successful in this area. Digital / mobile wallet payments represent around 27% of e-commerce payments in Europe, 36% in India and 69% in Asia.

Not only do payments feed into their “DNA loop”, but big techs helped turn payments into a glittering business, with e-commerce and social media offering opportunities for innovations to prosper.

The value of cashless payments consequently increased by 15% in 2021 in both advanced and emerging economies, even more quickly than the trend of the last decade, and this acceleration is expected to continue in the next few years, notably for wallets.

Big techs were then considered major competitors of banks and financial institutions – and sometimes even central banks.

In 2019, Facebook unveiled its Libra project that consisted of issuing stablecoins pegged to several currencies, claiming cheap and efficient payment solutions (including for cross-border payments) and greater financial inclusion.

Around the same time the strange word "cryptocurrencies" appeared, a word that hurt the ears of politicians and central bankers. From time immemorial, money had been sovereign in order to be reliable and lasting.

B. Disappointing learning years?

Needless to say Libra had its risks. I will not list them all, but it raised very significant concerns about financial stability, money laundering, etc.

The issues at stake reached far beyond mere financial regulation, and also included more acutely than ever the question of competition.

This is when big techs entered their learning years in finance, confronting reality.

Libra did not materialise, even after it was adjusted and rebranded as Diem.

Existing stablecoins are issued by players other than big techs, mainly from the digital asset industry.

Incidentally, after the failures and/or crimes committed by some of them, it is high time to regulate cryptos in full and to require licensing.

Let us not kid ourselves into believing that we can count on the so called "crypto winter " which has actually lasted for over a year now, to make the problem disappear by itself. That would be a dangerous illusion and would further delay supervision that is so badly needed.

All jurisdictions agree in principle to regulate, under the common FSB umbrella. But let us not only write reports and elaborate ever more sophisticated thoughts, let us act, starting with comprehensive and effective regulation in the US, as has been done in Europe, and as the UK is on its way to doing with its proposed new set of rules that would bring a broad range of cryptoasset activities into the scope of financial services regulation.

This is obviously good news, as long as this proposal ensures consistency with existing legislation, notably in Europe. To that end, I suggest the FSB to monitor closely the implementation of its own recommendations on cryptos, as the Basel Committee does on banking regulations.

More broadly, big techs did not make the breakthrough in traditional banking activities that many had expected: why is that? Regulatory constraints certainly stand as a first explanation, especially since they were tightened following the great financial crisis.

Both lending and deposit-taking are highly regulated in most advanced economies, and big techs tend to set up partnerships with banks in these countries rather than create a fully-owned subsidiary for instance.

In addition, the low-rate environment that prevailed until recently may have been unfavourable to new banks – as their business model relies strongly on the value of sight deposits –, and an ageing population in advanced economies may have preserved loyalty to incumbent banks and insurance companies which benefit from high public trust.

For the first time, big techs may now be touching on the limits of their core business models, and might seek further diversification, as financial activities already account for around 11% of their revenues.

So the question is: will this breakthrough in finance happen at all? Time will tell, but in my view, disintermediation by big techs remains a plausible scenario. The massive and prosperous tech firms can learn from their difficulties and enter into the space of banking and finance.

This raises the question of the conditions under which big techs could broaden their reach.

To read more:
https://www.banque-france.fr/en/intervention/big-techs-finance-bildungsroman-far-over

Big techs in finance: forging a new regulatory path

Agustín Carstens, General Manager, Bank for International Settlements, at the BIS conference "Big techs in finance – implications for public policy", Basel, Switzerland.

It is my great privilege to welcome you today to the BIS conference on big techs in finance – implications for public policy.

This high-level conference brings together prominent officials from international bodies, central banks and supervisory authorities, as well as renowned academics and private sector representatives.

It will provide a unique forum to exchange views on the most pressing policy challenges associated with big techs' involvement in the financial sector.

Current circumstances have allowed us to invite you to join us in person here in Basel, and it gives me great pleasure to see many of you could accept our invitation. Of course, let me also welcome those of you who are joining us remotely today.

Big techs and data

We at the BIS have been closely following large technology firms (big techs) and their advances into finance. Big techs' reach extends across a wide range of industries, with existing core businesses grounded in e-commerce and social media, among others. From this base, they have expanded into finance.

To understand how big techs can easily make forays into finance, one must grasp the key role of data. Indeed, big techs have fully embraced the centrality of data in the digital economy. This is what distinguishes them from other firms. It also shapes their unique characteristics. Let me mention those that are particularly relevant for policymakers.

First, big techs can overcome limits to scale in financial services provision by using user data from their existing businesses. Their business model revolves around users' direct interactions and the data generated as a by-product of these interactions. They use that data to offer a range of

services that exploit the inherent network effects in digital services, a phenomenon where more users attract ever more users.

In this way, big techs can establish a substantial presence in financial services very quickly through what we call the "data-network-activities" (DNA) loop.

Second, big techs collect different types of data from the various business lines they straddle. They are uniquely positioned to combine that data to uncover patterns and insights that can help them improve their services or offer new ones.

This combination of different types of data across sectors carries efficiency gains and is key to big techs' provision of digital services.

Third, big techs are unrivalled experts in data management and analysis. They devote significant resources to developing or acquiring state-of-the-art technologies. After all, access to large troves of data generates value only if you also have the technological capabilities to analyse it and monetise it.

Big techs have been pioneers in leveraging artificial intelligence techniques for this purpose.

To be sure, these capabilities have high fixed costs, but once that is overcome the marginal cost of handling more data is negligible. Therefore, big techs benefit from significant economies of scale in their use of data.

For other firms, reaping the benefits of such economies of scale is a tall order. Data management is thus at the core of big tech activities, and the financial sector is all about managing information. Coupled with big techs' relentless drive to expand, their growing and already substantial footprint in financial services should come as no surprise.

Moreover, the trend towards greater digitalisation, which the Covid-19 pandemic has accelerated, has allowed big techs to fortify their market positions even further.

Public policy challenges

Given their size and customer reach, big techs' entry into finance could trigger rapid change in the industry, generating both opportunities and challenges.
The potential benefits of big techs' entry into finance include improved customer outcomes, increased financial market efficiency and enhanced financial inclusion.

For example, BIS research has shown that access to innovative (QR code-based) payment methods provided by big techs helps micro firms build up credit history, and the use of big tech credit can ease access to bank credit. And there are many more examples.

To read more: https://www.bis.org/speeches/sp230208.pdf

Implementation of G20 Non-Bank Financial Intermediation Reforms, Progress report

FSB FINANCIAL STABILITY BOARD

This report describes progress in implementing reforms that had been agreed by the G20 following the 2008 global financial crisis to strengthen the oversight and regulation of non-bank financial intermediation (NBFI). The implementation status in various NBFI areas is as follows:

1. Jurisdictions have made progress in implementing Basel III reforms to mitigate spillovers between banks and non-bank financial entities, but implementation is not yet complete.

Four jurisdictions have yet to implement applicable risk-based capital requirements for banks' investments in the equity of funds or the supervisory framework for measuring and controlling banks' large exposures.

2. Adoption of the 2012 IOSCO recommendations to reduce the run risk of money market funds (MMFs) is most advanced in the largest MMF markets.

All FSB members adopted the fair value approach for valuation of MMF portfolios, though one jurisdiction does not have in place requirements for use of the amortised cost method only in limited circumstances.

Progress in liquidity management is less advanced. An IOSCO review found that the policy measures in nine jurisdictions representing about 95% of global net MMF assets are generally in line with the IOSCO recommendations.

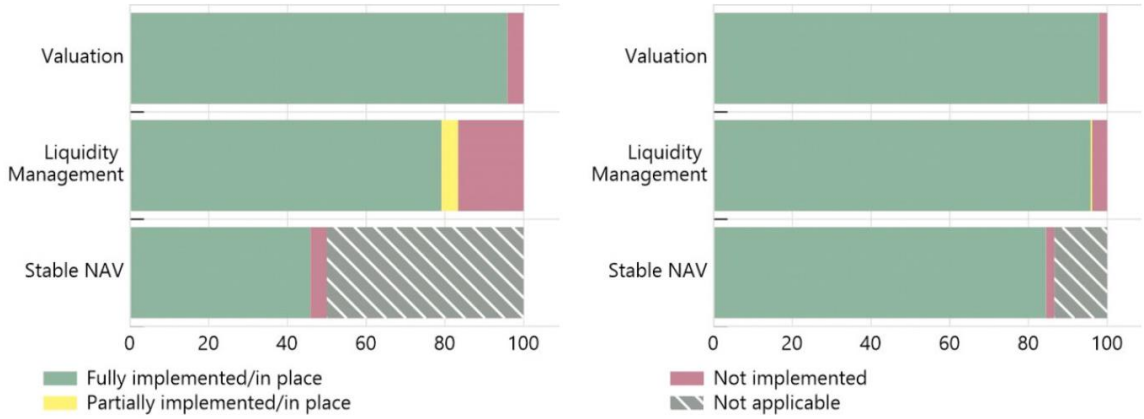
3. Adoption of the IOSCO recommendations on incentive alignment approaches for securitisation and of the BCBS standard on revised securitisation framework is ongoing.

About one-third of FSB jurisdictions (for the IOSCO recommendations) and one-sixth of FSB jurisdictions (for the BCBS standard) have yet to implement them.

4. Implementation of FSB recommendations for dampening procyclicality and other financial stability risks associated with securities financing transactions (SFTs) is incomplete and continues to face significant delays in most jurisdictions.

On global SFT data collection and aggregation, a few FSB jurisdictions are submitting data to the BIS.

Implementation progress is most advanced in the largest MMF markets Graph 1



[1] The five EU members of the FSB are presented as separate jurisdictions. [2] Market size based on assets under management (AUM) in FSB jurisdictions at end-2020.

5. Implementation of most FSB recommendations to assess and mitigate systemic risks posed by other non-bank financial entities and activities is ongoing.

The FSB and IOSCO assessed the implementation and effectiveness of their respective recommendations to address liquidity mismatch in open-ended funds (OEFs).

The FSB found that authorities have made meaningful progress in implementing the 2017 FSB Recommendations, but that lessons learnt since then have produced new insights into liquidity management challenges in segments of the OEF sector.

While the assessment suggests that the FSB Recommendations remain broadly appropriate, enhancing clarity and specificity on the policy outcomes the FSB Recommendations seek to achieve would make them more effective from a financial stability perspective.

IOSCO's review of its 2018 Recommendations shows a high degree of implementation of regulatory requirements consistent with the Recommendations' objectives, but some areas may warrant further attention. In addition to these reforms, the FSB is carrying out further analytical and policy work to enhance the resilience of the NBFI sector, building on the lessons from the March 2020 market turmoil.

To read more: https://www.fsb.org/wp-content/uploads/P180123.pdf

BIS Working Papers, No 1070

Theory of supply chains: a working capital approach

by Se-Jik Kim and Hyun Song Shin, Monetary and Economic Department

Abstract

This paper presents a time-to-build theory of supply chains which implies a key role for the financing of working capital as a determinant of supply chain length. We apply our theory to offshoring and trade, where firms strike a balance between the productivity gain due to off-shoring against the greater financial cost due to longer supply chains. In equilibrium, the ratio of trade to GDP, inventories and productivity are procyclical and closely track financial conditions.

Introduction

Production takes time, especially when conducted through long supply chains.

Working capital in the form of inventories and receivables bridges the timing mismatch between incurring costs and receiving cash from sales. To the extent that the financing cost of working capital matters, the length of supply chains is not only a matter of the economic fundamentals (such as the production technology or trade barriers) but is also shaped by financial conditions.

In this paper, we lay out a theory of supply chains where financial conditions play a pivotal role in the determination of the length of supply chains.

Through this theory, we highlight a novel channel for macro fluctuations through investment in working capital, which bears a strong analogy with investment in physical capital, but which operates across groups of firms, rather than at the individual firm level.

We highlight the associated repercussions of financing conditions on productivity and the volume of international trade.

By highlighting the analogy between physical capital and working capital on the firms balance sheet, our theory suggests a reorientation in the way that economists think of inventories.
Rather than being a buffer stock that smooths shocks, inventories in transit reflect the choice in working capital investment underpinning global supply chains.

Tom Friedman's (2005) popular book on globalization ("The World is Flat") has an apt quote from the chief executive of UPS in this respect. The UPS CEO is quoted as saying:

"When our grandfathers owned shops, inventory was what was in the back room. Now it is a box two hours away on a package car, or it might be hundreds more crossing the country by rail or jet, and you have thousands more crossing the ocean" [Friedman (2005, p. 174)]

To read more: https://www.bis.org/publ/work1070.pdf

Countercyclical capital buffer

ESRB
European Systemic Risk Board
European System of Financial Supervision

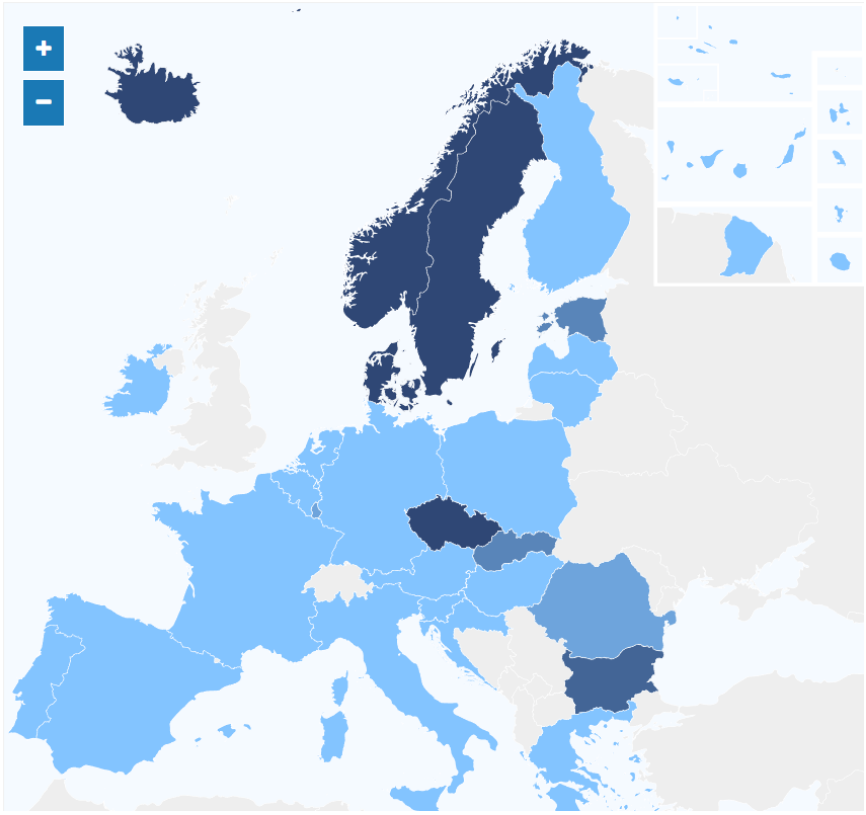
The countercyclical capital buffer (CCyB) is designed to counter procyclicality in the financial system.

When cyclical systemic risk is judged to be increasing, institutions should accumulate capital to create buffers that strengthen the resilience of the banking sector during periods of stress when losses materialise.

This will help maintain the supply of credit to the economy and dampen the downswing of the financial cycle. The CCyB can also help dampen excessive credit growth during the upswing of the financial cycle.

Please consult the respective national authorities' websites for the most up-to-date information. The tables below will be updated after the ESRB has received official notifications of the measures (last updated: 10 January 2023).

The following map shows current CCyB rates set (i.e. after the 12-month phase-in period) in Europe:



Country	Implementation date	Current CCyB
Austria	1 Jan 2016	0%
Belgium	1 Apr 2020	0%
Bulgaria	1 Jan 2023	1.5%
	1 Oct 2023	2%
Croatia	1 Jan 2016	0%
	31 Mar 2023	0.5%
	31 Dec 2023	1%
Cyprus	1 Jan 2016	0%
	30 Nov 2023	0.5%
Czech Republic	1 Jan 2023	2%
	1 Apr 2023	2.5%
Denmark	31 Dec 2022	2%
	31 Mar 2023	2.5%
Estonia	7 Dec 2022	1%
	1 Dec 2023	1.5%
Finland	16 Mar 2015	0%
France	1 Apr 2020	0%
	7 Apr 2023	0.5%
	2 Jan 2024	1%
Germany	1 Apr 2020	0%
	1 Feb 2023	0.75%
Greece	1 Jan 2016	0%
Hungary	1 Jan 2016	0%
	1 Jul 2023	0.5%
Iceland	29 Sep 2022	2%
Ireland	1 Apr 2020	0%
	15 Jun 2023	0.5%
Italy	1 Jan 2016	0%
Latvia	1 Feb 2016	0%
Liechtenstein	1 Jul 2019	0%
Lithuania	1 Apr 2020	0%
	1 Oct 2023	1%
Luxembourg	1 Jan 2021	0.5%
Malta	1 Jan 2016	0%
Netherlands	1 Jan 2016	0%
	25 May 2023	1%
Norway	31 Dec 2022	2%
	31 Mar 2023	2.5%
Poland	1 Jan 2016	0%
Portugal	1 Jan 2016	0%
Romania	17 Oct 2022	0.5%

To read more:
https://www.esrb.europa.eu/national_policy/ccb/html/index.en.html

The NIS 2 Directive of the EU

EUR-Lex
Access to European Union law

Network and information systems have developed into a central feature of everyday life with the speedy digital transformation and interconnectedness of society, including in cross-border exchanges.

That development has led to an expansion of the cyber threat landscape, bringing about new challenges, which require adapted, coordinated and innovative responses in all Member States.

The number, magnitude, sophistication, frequency and impact of incidents are increasing, and present a major threat to the functioning of network and information systems.

As a result, incidents can impede the pursuit of economic activities in the internal market, generate financial loss, undermine user confidence and cause major damage to the Union's economy and society.

Cybersecurity preparedness and effectiveness are therefore now more essential than ever to the proper functioning of the internal market.

Moreover, cybersecurity is a key enabler for many critical sectors to successfully embrace the digital transformation and to fully grasp the economic, social and sustainable benefits of digitalisation.

The cybersecurity requirements imposed on entities providing services or carrying out activities which are economically significant vary considerably among Member States in terms of type of requirement, their level of detail and the method of supervision.

Those disparities entail additional costs and create difficulties for entities that offer goods or services across borders.

Requirements imposed by one Member State that are different from, or even in conflict with, those imposed by another Member State, may substantially affect such cross-border activities.

Furthermore, the possibility of the inadequate design or implementation of cybersecurity requirements in one Member State is likely to have repercussions at the level of cybersecurity of other Member States, in particular given the intensity of cross-border exchanges.

The review of Directive (EU) 2016/1148 has shown a wide divergence in its implementation by Member States, including in relation to its scope, the

delimitation of which was very largely left to the discretion of the Member States.

Directive (EU) 2016/1148 also provided the Member States with very wide discretion as regards the implementation of the security and incident reporting obligations laid down therein.

Those obligations were therefore implemented in significantly different ways at national level.

There are similar divergences in the implementation of the provisions of Directive (EU) 2016/1148 on supervision and enforcement.

All those divergences entail a fragmentation of the internal market and can have a prejudicial effect on its functioning, affecting in particular the cross-border provision of services and the level of cyber resilience due to the application of a variety of measures.

Ultimately, those divergences could lead to the higher vulnerability of some Member States to cyber threats, with potential spill-over effects across the Union.

This Directive aims to remove such wide divergences among Member States, in particular by setting out minimum rules regarding the functioning of a coordinated regulatory framework, by laying down mechanisms for effective cooperation among the responsible authorities in each Member State, by updating the list of sectors and activities subject to cybersecurity obligations and by providing effective remedies and enforcement measures which are key to the effective enforcement of those obligations.

Therefore, Directive (EU) 2016/1148 should be repealed and replaced by this Directive.

With the repeal of Directive (EU) 2016/1148, the scope of application by sectors should be extended to a larger part of the economy to provide a comprehensive coverage of sectors and services of vital importance to key societal and economic activities in the internal market.

In particular, this Directive aims to overcome the shortcomings of the differentiation between operators of essential services and digital service providers, which has been proven to be obsolete, since it does not reflect the importance of the sectors or services for the societal and economic activities in the internal market.

To read more: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

27.12.2022 | EN | Official Journal of the European Union | L 333/80

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

(Text with EEA relevance)

Federal Reserve Board announces denial of application by Custodia Bank, Inc. to become a member of the Federal Reserve System

The Federal Reserve Board announced its denial of the application by Custodia Bank, Inc., Cheyenne, Wyoming, to become a member of the Federal Reserve System.

The Board has concluded that the firm's application as submitted is inconsistent with the required factors under the law.

Custodia is a special purpose depository institution, chartered by the state of Wyoming, which does not have federal deposit insurance.

The firm proposed to engage in novel and untested crypto activities that include issuing a crypto asset on open, public and/or decentralized networks.

The firm's novel business model and proposed focus on crypto-assets presented significant safety and soundness risks.

The Board has previously made clear that such crypto activities are highly likely to be inconsistent with safe and sound banking practices.

The Board also found that Custodia's risk management framework was insufficient to address concerns regarding the heightened risks associated with its proposed crypto activities, including its ability to mitigate money laundering and terrorism financing risks.

In light of these and other concerns, the firm's application as submitted was inconsistent with the factors the Board is required to evaluate by law.

The Board's order will be released following a review for confidential information.

To read more:
https://www.federalreserve.gov/newsevents/pressreleases/orders20230127a.htm

Engineering Personal Data Sharing

This report attempts to look closer at specific use cases relating to personal data sharing, primarily in the health sector, and discusses how specific technologies and considerations of implementation can support the meeting of specific data protection.

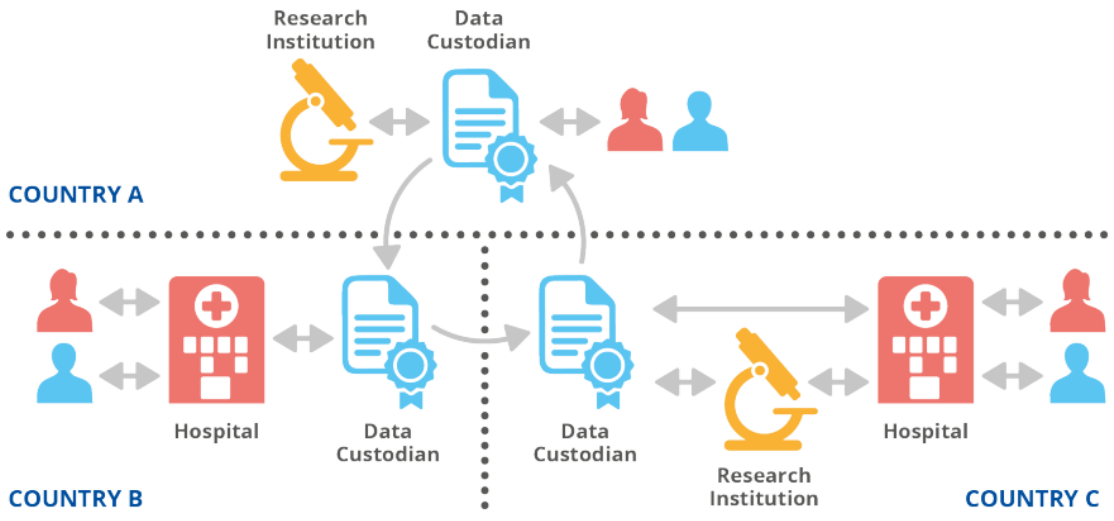
After discussing some challenges in (personal) data sharing, this report demonstrates how to engineer specific technologies and techniques in order to enable privacy preserving data sharing.

More specifically it discusses specific use cases for sharing data in the health sector, with the aim of demonstrating how data protection principles can be met through the proper use of technological solutions relying on advanced cryptographic techniques.

Next it discusses data sharing that takes place as part of another process or service, where the data is processed through some secondary channel or entity before reaching its primary recipient.

Lastly, it identifies challenges, considerations and possible architectural solutions on intervenability aspects (such as the right to erasure and the right to rectification when sharing data).

Figure 17: Cross border data exchange with data custodians



When two or more parties decide to share their data, they become part of a larger data ecosystem where they can take advantage of the combined data set that enables the discovery, by way of computation, of new information

or trends relating to individuals, groups of individuals, or to society as a whole.

The easiest and most straightforward way to achieve this goal would be to exchange the raw data that each actor holds across technical interfaces putting them on a common table (i.e. a single database) but this hypothetical option is not really feasible.

In reality we are pursuing trusted sharing environments that will make full use of the potential offered by a safe and secure exchange and use of personal data while respecting data protection principles.

This report attempted to look closer at specific use cases relating to personal data sharing, primarily in the health sector, and to discuss how specific technologies and considerations of implementation can support the engineering of personal data sharing in practice.

The analysis ranged from user-controlled data sharing to large scale personal data gathering and data sharing using third party service.

Despite the potential of the data sharing concept and the relevant Union policy and law in the area, there are still considerations on which are the appropriate technical and organizational measures and how to engineer them into practice.

The European legislative initiatives on data sharing described in Section 1.1 entail the processing of large quantities of data which will also include personal data.

Therefore, in addition to the consistency of their provisions with the GDPR, it is important to remove any legal uncertainty on the roles and obligations, not only for individuals as highlighted by the EDPB and the EDPS but also for the entities involved in the data sharing.

In order to leverage the potential of data sharing across the EU, practitioners could be provided with directions on which technologies and techniques can be considered, under which circumstances and which data protection principles can be met.

There are several commonly used (cryptographic) techniques (i.e. asymmetric encryption, pseudonyms, access control etc) that are already acknowledged as able to alleviate data protection risks.
Some of them were discussed in Section 2, Section 3 and Section 4. In emerging concepts such as data spaces and data intermediaries, however, the risks introduced cannot always be adequately addressed only by such techniques.

This is due to the fact that data subjects want to preserve confidentiality of the data they are sharing, they might not know beforehand with whom they might be sharing data with or might want to share accumulated datasets.

Although there are advanced techniques that are still evolving, they should not be considered as of purely academic interest since there exist practical implementations in real use case scenarios.

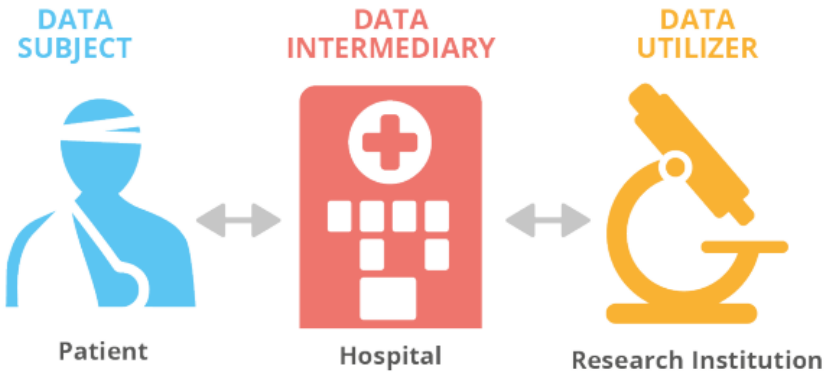
Lastly, since the majority of the technologies described earlier and in previous ENISA reports rely on asymmetric cryptography, the advent of quantum computing and the impact on the security of currently used asymmetric ciphers should be anticipated.

Following the deployment of data sharing infrastructures and services, we cannot expect that they will cease to operate due to possible inadequacy of the asymmetric ciphers.

This is where crypto agility becomes relevant as it allows for a switch between algorithms, cryptographic primitives, and other encryption mechanisms without significant changes in the overall IT system or process.

To read more:
https://www.enisa.europa.eu/publications/engineering-personal-data-sharing

Figure 14: Data sharing scenario with data intermediaries



Think before you link

CPNI
Centre for the Protection of National Infrastructure

Have you ever encountered someone online who was not who they seemed?

In the digital age, online social and professional networking sites are enabling us to be more joined up than ever, but also expose us to unforeseen risks.

Our app can help keep you, your colleagues, and the country safe from being targeted by malicious profiles online.

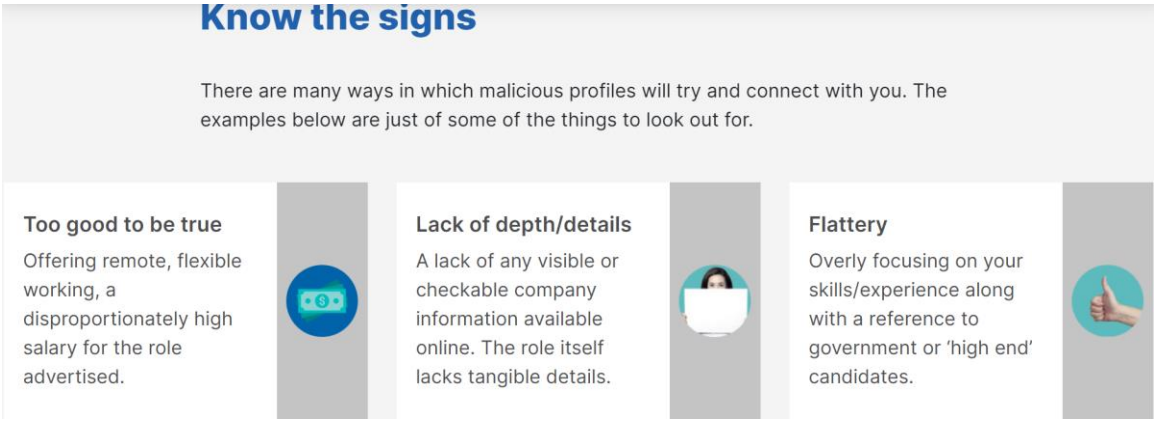
The Think Before You Link campaign, on which this app is based, is designed to raise awareness of the threat posed by hostile state actors and organised criminals from trying to steal intellectual property or information through social media and professional networking sites.

How do they trick you?

Typically, hostile actors and criminals contact the target posing as an interested 'employer' or recruitment consultant presenting a unique business opportunity.

They ask for further details about the target's background, try to "sell" the business opportunity, and insist on discussing it privately, away from the initial website.
This kind of engagement is an attempt to understand the level of access the individual has to sensitive information, draw it out from them, and build a longer term relationship.

Most of the time the target is not aware of the real purpose of the approach. In some instances, they believe they are providing information to develop a legitimate business opportunity.



About CPNI

CPNI is the government authority for protective security advice to the UK national infrastructure. Our role is to protect national security by helping to reduce the vulnerability of the national infrastructure to terrorism and other threats. We are accountable to the Director General of MI5.

There are also other nationally important assets or events, including high-profile iconic targets, where impact of damage would be equally serious even though these do not deliver an essential service. Our advice delivery extends to help the protection of such assets and events.

CPNI is committed to equality, diversity and inclusion (EDI). EDI is integral to our culture and working practices, as well as our protective security efforts. We also work closely with key partners to promote greater EDI in the wider security profession.

To read more: https://thinkbeforeyoulink.app

SEC Publishes Annual Staff Report on Nationally Recognized Statistical Rating Organizations

The Securities and Exchange Commission published a staff report that provides a summary of the staff's examinations of nationally recognized statistical rating organizations (NRSROs) and discusses the state of competition, transparency, and conflicts of interest among NRSROs.

"The Office of Credit Ratings is critical to the Commission's work to protect investors and ensure the integrity of the rating process, including through the office's oversight of Nationally Recognized Statistical Rating Organizations," said SEC Chair Gary Gensler.

"Through the 2022 staff report, the OCR continues its work to ensure credit ratings are accurate, reliable, and fair."

"Our risk-based approach to NRSRO examinations protects investors by focusing on specific NRSRO activities and assessing compliance with applicable laws and rules," said Lori Price, Director of the Office of Credit Ratings. "The comprehensive staff report summarizes the findings from our annual examinations and also provides information about NRSROs, their credit ratings businesses, and the industry more broadly."

As described in the report, the staff's NRSRO examinations during 2022 considered a number of factors, including:

- Rating surveillance practices;

- The impact of COVID-19 on commercial real estate credit ratings;

- Whether business communications are conducted through unauthorized means;

- Securities ownership by NRSRO employees;

- The effect on credit ratings from the marketing and development of stand-alone ESG products; and

- Ratings of firms based in China.

- Prior years' reports from the Office of Credit Ratings are available here.

To read more: https://www.sec.gov/files/2023-ocr-staff-report.pdf

Chart 1. Table of NRSROs

NRSRO	Categories of Credit Ratings	Principal Office
A.M. Best Rating Services, Inc. (AMB)	(ii), (iii), and (iv)	U.S.
DBRS, Inc. (DBRS)	(i) through (v)	U.S.
Demotech, Inc. (Demotech)	(ii)	U.S.
Egan-Jones Ratings Company (EJR)	(i) through (iii)	U.S.
Fitch Ratings, Inc. (Fitch)	(i) through (v)	U.S.
HR Ratings de México, S.A. de C.V. (HR)	(i), (iii), and (v)	Mexico
Japan Credit Rating Agency, Ltd. (JCR)	(i), (ii), (iii), and (v)	Japan
Kroll Bond Rating Agency, LLC (KBRA)	(i) through (v)	U.S.
Moody's Investors Service, Inc. (Moody's)	(i) through (v)	U.S.
S&P Global Ratings (S&P)	(i) through (v)	U.S.

Phishing Resistance – Protecting the Keys to Your Kingdom

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

If you own a computer, watch the news, or spend virtually any time online these days you have probably heard the term “phishing.” Never in a positive context…and possibly because you have been a victim yourself.

Phishing refers to a variety of attacks that are intended to convince you to forfeit sensitive data to an imposter.

These attacks can take a number of different forms; from spear-phishing (which targets a specific individual within an organization), to whaling (which goes one step further and targets senior executives or leaders).

Furthermore, phishing attacks take place over multiple channels or even across channels; from the more traditional email-based attacks to those using voice – vishing – to those coming via text message – smishing.

Regardless of the type or channel, the intent of the attack is the same – to exploit human nature to gain control of sensitive information.

These attacks typically make use of several techniques including impersonated websites, attacker-in-the-middle, and relay or replay to achieve their desired outcome.

Due to their effectiveness and simplicity, phishing attacks have rapidly become the tool of choice for baddies everywhere.

As a tactic, it is used by everyone from low level criminals looking to commit fraud, to the sophisticated nation state attackers seeking a foothold within an enterprise network. And, while almost any kind of information can be targeted, often the most damaging attacks focus on your password, pin, or one-time passcodes – the keys to your digital realm.

The combination can be catastrophic. The Verizon 2022 Data Breach Investigations Report lists phishing and stolen credentials (which may be harvested during phishing attacks) as two of the four “key pathways” that organizations must be prepared to address in order to prevent breaches.

In recognition of the threat posed by phishing – the Office of Management and Budget’s Memo 22-09 “Moving the U.S. Government Toward Zero Trust Cybersecurity Principles” prioritizes implementation of phishing resistant authenticators.

You may visit:
https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

January 26, 2022

M-22-09

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director

SUBJECT: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

This memorandum sets forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 in order to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns. Those campaigns target Federal technology infrastructure, threatening public safety and privacy, damaging the American economy, and weakening trust in Government.

So – how do you keep your keys from falling into the wrong hands? What constitutes a phishing resistant authenticator?

NIST Special Publication DRAFT 800-63-B4 defines it as "the ability of the authentication protocol to detect and prevent disclosure of authentication secrets and valid authenticator outputs to an impostor relying party without reliance on the vigilance of the subscriber." To achieve this, phishing resistant authenticators must address the following attack vectors associated phishing:

1. Impersonated Websites – Phishing resistant authenticators prevent the use of authenticators at illegitimate websites (known as verifiers) through multiple cryptographic measures.

This is achieved through the establishment of authenticated protected channels for communications and methods to restrict the context of an authenticator's use.

For example, this may be achieved through name binding – where an authenticator is only valid for a specific domain (I can only use this for one website). It may also be achieved through binding to a communication channel – such as in client authenticated TLS (I can only use this over a specific connection).

2. Attacker-in-the Middle - Phishing resistant authenticators prevent an attacker-in-the-middle from capturing authentication data from the user and relaying it to the relying website.

This is achieved through cryptographic measures, such as leveraging an authenticated protected channel for the exchange of information and digitally signing authentication data and messages.

3. User Entry – Phishing resistant authenticators eliminate the need for a user to type or manually input authentication data over the internet.

This is achieved through the use of cryptographic keys for authentication that are unlocked locally through a biometric or pin. No user entered information is exchanged between the relying website and the authenticator itself.

4. Replay – Phishing resistant authenticators prevent attackers from using captured authentication data at a later point in time.

Supporting cryptographic controls for restricting context and to prevent attacker-in-the-middle scenarios are also preventative of replay attacks, particularly digitally signed and time-stamped authentication and message data.

As complicated as this may seem, there are several practical examples of phishing resistant authenticators in place today.

For U.S. federal employees, the most ubiquitous form of phishing resistant authenticator is the Personal Identity Verification (PIV) card; they leverage public-key cryptography to protect authentication events.

Commercially, FIDO authenticators paired with W3C's Web Authentication API are the most common form of phishing resistant authenticators widely available today.

These can take the form of separate hardware keys or be embedded directly into platforms (for example your phone or laptop).
Availability, practicality, and security of these "platform authenticators" increasingly puts strong, phishing resistant authenticators into user's hands without the need for additional form factors or dongles.

Not every transaction requires phishing resistant authenticators. However, for applications that protect sensitive information (such as health information or confidential client data) or for users that have elevated privileges (such as admins or security personnel) organizations should be enforcing, or at least offering, phishing resistant authenticators.

Individuals should explore the security settings for their more sensitive online accounts to see if phishing resistant authenticators are available and make use of them if they are. In reality, these tools are often easier, faster, and more convenient than the MFA – such as SMS text codes – they may currently be using.

In the end, phishing resistant authenticators are a critical tool in personal and enterprise security that should be embraced and adopted. They are not, however, a silver bullet.

Phishing resistant authenticators only address one focus of phishing attacks – the compromise and re-use of authenticators such as passwords and one-time passcodes.

They do not mitigate phishing attempts that may have alternative goals such as installing malware or compromising personal information to be used elsewhere.

Phishing resistant authenticators should be paired with a comprehensive phishing prevention program that includes user awareness and training, email protection controls, data loss prevention tools, and network security capabilities.

To read more:
https://www.nist.gov/blogs/cybersecurity-insights/phishing-resistance-protecting-keys-your-kingdom

Kraken to Discontinue Unregistered Offer and Sale of Crypto Asset Staking-As-A-Service Program and Pay $30 Million to Settle SEC Charges

The Securities and Exchange Commission charged Payward Ventures, Inc. and Payward Trading Ltd., both commonly known as Kraken, with failing to register the offer and sale of their crypto asset staking-as-a-service program, whereby investors transfer crypto assets to Kraken for staking in exchange for advertised annual investment returns of as much as 21 percent.

To settle the SEC's charges, the two Kraken entities agreed to immediately cease offering or selling securities through crypto asset staking services or staking programs and pay $30 million in disgorgement, prejudgment interest, and civil penalties.

According to the SEC's complaint, since 2019, Kraken has offered and sold its crypto asset "staking services" to the general public, whereby Kraken pools certain crypto assets transferred by investors and stakes them on behalf of those investors.

Staking is a process in which investors lock up – or "stake" – their crypto tokens with a blockchain validator with the goal of being rewarded with new tokens when their staked crypto tokens become part of the process for validating data for the blockchain.

When investors provide tokens to staking-as-a-service providers, they lose control of those tokens and take on risks associated with those platforms, with very little protection.

The complaint alleges that Kraken touts that its staking investment program offers an easy-to-use platform and benefits that derive from Kraken's efforts on behalf of investors, including Kraken's strategies to obtain regular investment returns and payouts

"Whether it's through staking-as-a-service, lending, or other means, crypto intermediaries, when offering investment contracts in exchange for investors' tokens, need to provide the proper disclosures and safeguards required by our securities laws," said SEC Chair Gary Gensler. "Today's action should make clear to the marketplace that staking-as-a-service providers must register and provide full, fair, and truthful disclosure and investor protection."

"In case after case, we've seen the consequences when individuals and businesses tout and offer crypto investments outside of the protections provided by the federal securities laws: investors lack the disclosures they deserve and are harmed when they don't receive them," said Gurbir S. Grewal, Director of the SEC's Division of Enforcement.

"Today, we take another step in protecting retail investors by shutting down this unregistered crypto staking program, through which Kraken not only offered investors outsized returns untethered to any economic realities, but also retained the right to pay them no returns at all. All the while, it provided them zero insight into, among other things, its financial condition and whether it even had the means of paying the marketed returns in the first place."

In addition to ceasing the staking program and the monetary relief, Payward Ventures, Inc. and Payward Trading, Ltd, without admitting or denying the allegations in the SEC's complaint, consented to the entry of a final judgment, subject to court approval, that would permanently enjoin each of them from violating Section 5 of the Securities Act of 1933 and permanently enjoin them and any entity they control from, directly or indirectly, offering or selling securities through crypto asset staking services or staking programs.

The SEC's investigation was conducted by Laura D'Allaird and Elizabeth Goody, under the supervision of Paul Kim, Jorge G. Tenreiro, and David Hirsch, with assistance from Sachin Verma, Eugene Hansen, and James Connor.

To read more: https://www.sec.gov/news/press-release/2023-25

Statement

Kraken Down: Statement on SEC v. Payward Ventures, Inc., et al.

SEC Commissioner Hester M. Peirce

Today, the SEC shut down Kraken's staking program and counted it as a win for investors. I disagree and therefore dissent.

Kraken operated a service through which its customers could offer their tokens up for staking. The customers earned returns, and the company earned a fee. The Commission argues that this staking program should have been registered with the SEC as a securities offering.

Whether one agrees with that analysis or not, the more fundamental question is whether SEC registration would have been possible. In the current climate, crypto-related offerings are not making it through the SEC's registration pipeline.

An offering like the staking service at issue here raises a host of complicated questions, including whether the staking program as a whole would be registered or whether each token's staking program would be separately registered, what the important disclosures would be, and what the accounting implications would be for Kraken.

We have known about crypto staking programs for a long time. Although it may not have made a difference, I should have called for us to put out guidance on staking long before now.

Instead of taking the path of thinking through staking programs and issuing guidance, we again chose to speak through an enforcement action, purporting to "make clear to the marketplace that staking-as-a-service providers must register and provide full, fair, and truthful disclosure and investor protection."

Using enforcement actions to tell people what the law is in an emerging industry is not an efficient or fair way of regulating.

Moreover, staking services are not uniform, so one-off enforcement actions and cookie-cutter analysis does not cut it.
Most concerning, though, is that our solution to a registration violation is to shut down entirely a program that has served people well. The program will

no longer be available in the United States, and Kraken is enjoined from ever offering a staking service in the United States, registered or not.

A paternalistic and lazy regulator settles on a solution like the one in this settlement: do not initiate a public process to develop a workable registration process that provides valuable information to investors, just shut it down.

More transparency around crypto-staking programs like Kraken's might well be a good thing. However, whether we need a uniform regulatory solution and if that regulatory solution is best provided by a regulator that is hostile to crypto, in the form of an enforcement action, is less clear.

To read more:
https://www.sec.gov/news/statement/peirce-statement-kraken-020923

Disclaimer

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

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

This information:

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

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

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

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

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

- is in no way constitutive of an interpretative document;

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

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

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

It is our goal to minimize disruption caused by technical errors. However some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

The Association accepts no responsibility with regard to such problems incurred as a result of using this site or any linked external sites.

Basel iii Compliance Professionals Association (BiiiCPA)

The Basel iii Compliance Professionals Association (BiiiCPA) is the largest association of Basel iii Professionals in the world. It is a business unit of the Basel ii Compliance Professionals Association (BCPA), the largest association of Basel ii Professionals in the world.

We invite you to connect with the global community of experts working for the implementation of the Basel III framework, to gain insight into the G20 efforts to regulate the global financial system, to explore new career avenues, and most of all, to acquire lifelong skills.

You can explore what we offer to our members:

1. Membership - Become a standard, premium or lifetime member.
You may visit:
https://www.basel-iii-association.com/How_to_become_member.htm

2. Monthly Updates – Visit the Reading Room of the association at:
https://www.basel-iii-association.com/Reading_Room.html

3. Training and Certification – You may visit:
https://www.basel-iii-association.com/Basel_III_Distance_Learning_Online_Certification.html

For instructor-led training, you may contact us. We tailor Basel III presentations, awareness and training programs for supervisors, boards of directors, service providers and consultants.