INTERNATIONAL MONETARY FUND

IMF Country Report No. 24/42

CHILE

SELECTED ISSUES

February 2024

This paper on Chile was prepared by a staff team of the International Monetary Fund as background documentation for the periodic consultation with the member country. It is based on the information available at the time it was completed on January 17, 2024.

Copies of this report are available to the public from

International Monetary Fund • Publication Services
PO Box 92780 • Washington, D.C. 20090
Telephone: (202) 623-7430 • Fax: (202) 623-7201
E-mail: publications@imf.org Web: http://www.imf.org
Price: $18.00 per printed copy

International Monetary Fund
Washington, D.C.

INTERNATIONAL MONETARY FUND

CHILE

SELECTED ISSUES

January 17, 2024

Approved By
Western Hemisphere Department

Prepared By Si Guo (WHD) and Tatsushi Okuda (MCM).

CONTENTS

BOXES

BOXES

Figures

FIGURES

RENEWABLE ENERGY—AN ATTEMPT TO ESTIMATE THE GDP IMPACT AND ASSESS THE ROLE OF POLICIES[1]

Chile has a comparative advantage in renewable energy. Staff estimates show that replacing coal power with solar and wind power, as announced by the government, could boost the long-term GDP level by at least 1 percentage point. An additional benefit is the greater economic resilience to abrupt increases in coal and fuel prices that can have large negative impacts on the economy. A key constraint for the renewable energy sector is currently the transmission from where it is produced to where it is used. A cost-benefit analysis shows that state support for certain industries, such as electricity transmission, may have economic benefits that outweigh the costs.

A. Renewable Energy Power in Chile

1. **Chile has a comparative advantage in renewable energy.** The high solar radiation in the north and the strong winds in the south are ideal for solar and wind power generation. From 2010 to 2021, wind and solar power as a share of the total electricity supply increased from 1 to 20 percent. The total generation capacity from solar and wind could be up to about 1,800 GW, more than 70 times the total capacity installed as of 2021, according to the Ministry of Energy (2020).

Chile: Share of Electricity Supply by Energy Source

(In percent)

	Coal	Oil	Natural gas	Biofuels	Hydro	Wind	Solar PV
2005	14	6	26	3	50	0	0
2010	28	14	18	4	36	1	0
2015	37	4	15	7	32	3	2
2020	31	2	18	6	26	7	9
2021	30	5	18	7	19	8	12

Sources: IEA and IMF staff calculations.

2. **Electricity generation costs from solar and wind are lower than from fossil fuels in Chile.** The levelized costs of electricity (LOCEs)[2] were estimated to be USD 20-60 per MWH for solar generators and USD 40-50 per MWH for onshore wind generators in Chile (Zissler 2020). While the International Energy Agency (IEA) does not publish the LOCEs of coal-based electricity generators in Chile, data from other countries shows that the LOCEs of coal generators are in the range of USD 65-175 per MWh (IEA 2020) depending on installation technology, local coal prices, and carbon prices. The low production costs of solar and wind power are explained by two factors. First, the high

[1] Prepared by Si Guo. The author would like to thank the authorities for helpful discussions.

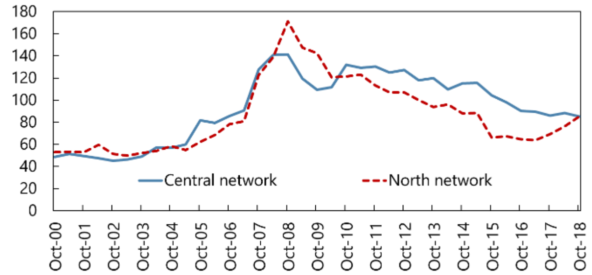
[2] Levelized cost of electricity (LCOE) is a measure of the annual production cost of electricity. LCOE is calculated as the sum of the net present value of capital expenditure and operating costs of electricity generation over the lifespan of the generator, divided by its expected lifetime. LOCEs depend on energy sources (e.g., solar or coal), locations, carbon taxes, and discount rates.

solar radiation and strong winds in Chile result in high energy capacity factors (CF) for solar and wind generators. Second, installation costs of solar and wind generators have declined substantially in the last decade (Feldman et al., 2020).

3. Over time, the average real electricity generation costs have declined substantially in Chile during 2008-21. This can be seen by dividing the annual real gross output of the electricity generation industry by electricity production volume, or more intuitively, by comparing the historical real electricity prices at node (text chart). There are three factors behind the decline. First, the natural gas shortage due to the export restrictions from Argentina during 2005-08 was largely relieved by 2010. Second, coal prices dropped during 2008-20, and coal power represents around 30 percent of the total electricity supply in Chile. Third, the increasing share of solar and wind generation and their declining installation costs drove down the average unit costs (Serra, 2022).

Chile: Real Electricity Price, 2000-18

(2019 USD per MWH)



Sources: Comision Nacional de Energia and IMF staff calculations.
Notes: The chart presents the average electricity prices (adjusted for U.S. CPI) for the two nodes in Chile's electricity systems: Crucero in the North network and Santiago in the Central network.

4. The bottleneck of further expanding electricity generation from solar and wind appears to be the mismatch between the geographic locations of generation and consumption. Chile has a long and narrow territory. The areas rich in solar and wind, namely the northern and southern parts of the country, are more than 1,000 miles away from the central area, the country's main economic hub. The difficulty in transmitting electricity to the end-consumption could lead to great price dispersion across regions, and in some circumstances, unused electricity. Gonzales et al. (2023) document that the completion of the North-South transmission lines in 2017 and 2019 lowered the regional electricity price dispersions and encouraged new investment in solar and wind generation projects.

5. The development of green hydrogen and its derivatives could potentially help overcome this mismatch. Hydrogen is an industrial intermediate input and a potential energy carrier. Green hydrogen refers to the hydrogen produced using renewable energy. This is opposed to "gray" hydrogen which relies on fossil fuels in the production process. Ideally, the electricity surplus in the renewable energy-intensive areas could be used to produce green hydrogen to overcome the geographic mismatch between electricity supply and demand.

6. The key obstacle to developing green hydrogen is its production costs. The costs mainly include electricity, desalinization, and electrolysers costs. Chile has an advantage in generating electricity from solar and wind at low costs, and the costs of electrolysers are likely to trend down when the production scale increases. However, more technology breakthroughs are still needed to make the production and transportation of green hydrogen economically viable.

B. The Impact of Renewable Power on GDP

7. How will the greater use of solar and wind power contribute to long-term GDP? The problem can be analyzed in two steps:

- *Productivity gain in electricity generation.* The continued increase in solar and wind power capacity will reduce the need for fossil fuels in electricity generation. Because the costs of electricity generation from solar and wind are lower than from fossil fuels, this transition can be considered as a productivity gain in the electricity generation industry.

- *Impact on GDP through the production network.* Higher productivity in the electricity generation industry will have direct and indirect effects on GDP. The direct effect is simply the higher value-added of the electricity generation industry as the result of its productivity increase. The indirect effect on GDP is from the inter-industry production linkages: a productivity increase in the electricity generation industry would affect its demand for intermediate inputs produced by industries and lower the electricity costs of other industries.

8. We estimate the long-term GDP gain under the working assumption that solar and wind power will completely replace coal. This assumption is consistent with Chile's target of retiring all coal power plants by 2040. For other sources of electricity supply (hydro, biofuels, gas, and oil), we assume that they will continue to grow at the same pace of the total energy supply, such that their shares in total the electricity supply will stay unchanged from 2021.[3]

Estimated Changes to the Electricity Generation Industry's Productivity

9. Replacing the more costly coal-based generators with less costly solar and wind generators represents a 28 percent increase in the electricity generation industry's productivity. We use IEA (2020) as the basis of our generation cost assumptions. IEA (2020) projects the levelized costs of electricity generation by country and generation method for (hypothetical) projects that will commission in 2025. Because Chile is not included in the projection sample of IEA (2020), we must impute the costs from other countries. The LCOE assumptions used in our exercise are listed in the text table. The implied weighted average LCOE for electricity generation based on Chile's energy structure in 2021 is about USD 68 per MWH. Because the LCOE for coal generation is USD 97 per MWH while the LCOEs for wind and solar-based generators are both USD 34 per MWH, replacing coal (which accounted for 30 percent of power generation in 2021) with wind and solar will save the electricity generation costs 28 percent (calculated as (97-34) * 30 percent / 68 = 28 percent).

[3] One potential caveat of this assumption is that the share of hydropower has been on a declining trend, in part because there were few new hydro projects. In an alternative scenario, we set the future hydropower generation level (in MWH) unchanged from its 2021 level. This would imply a declining share of hydropower in total electricity supply by 10 percentage points to be also filled by solar and wind power. The estimated productivity gain in the electricity generation industry in this alternative scenario is only slightly higher than the baseline scenario (30 percent versus 28 percent) because the cost difference between hydro and solar power is small and the scale of energy substitution (10 percent of total supply) is moderate.

Assumptions on Levelized Cost of Electricity Generation

(In U.S. dollars)

Generator Type	Cost per MWH	Notes
Coal	97	Based on IEA (2020) projection for Brazil
Oil	97	Imputed to be the same as coal
Natural Gas	79	Based on IEA (2020) projection for Brazil
Biofuels	54	Based on IEA (2020) projection for Brazil
Hydro	46	Based on IEA (2020) projection for Brazil
Wind	34	Based on IEA (2020) lowest projection for all countries
Solar	34	Based on IEA (2020) lowest projection for all countries
Weighted Average	68	

Sources: IEA (2020) and IMF staff calculations.

Estimated Impact on GDP

10. **We follow Hulten (1978) and Baqee and Farhi (2020) to estimate the impact of a productivity gain in electricity generation on aggregate GDP.** Estimating the aggregate GDP gain of a productivity increase in an industry typically requires a structural model and the estimates can sometimes be sensitive to production function assumptions. However, Hulten (1978) and Baqee and Farhi (2020) show that up to the first and second order approximations, the sufficient statistics for estimating the GDP gain are simply the gross output-to-GDP ratio of the industry and the change of this ratio in response to the industrial level productivity increase (Box 1).

Box 1. The Impact of Productivity Change in One Industry on Aggregate Productivity

Hulten (1978) shows that the sum of direct and indirect effects of an industry's productivity increase on aggregate productivity is determined by the industry's gross output-to-GDP share, up to the first-order approximation:

$$d\log(A)/d\log(A_k) = \lambda_k \qquad (1)$$

where *log(A$_k$)* is the percentage point increase in (Hicks-neutral) productivity of industry *k*. Parameter λ_k is the also called "Domar weight," which is defined as industry *k*'s total *gross output* (the sum of value-added and the value of intermediate inputs) divided by GDP. Equation (1) shows that even though the direct impact of industry *k*'s productivity growth on aggregate productivity is simply the increase in its value-added VA_k, the total productivity gain, including the indirect effects through the production network, is determined by industry *k*'s gross output-to-GDP ratio. That is, the difference between industry *k*'s gross output-to-GDP and value added-to-GDP ratios reflects the indirect effect through the inter-industry linkages.

Baqee and Farhi (2020) expand Hulten (1978) to second-order approximation:

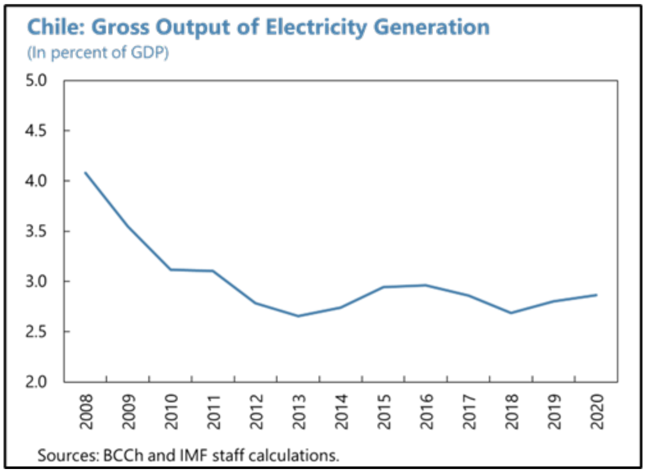
$$d\log(A)/d\log(A_k) = \lambda_k + \tfrac{1}{2}\,[d\lambda_k/d(\log A_k)]*d\log(A_k) \qquad (2)$$

The last term on the right-hand side of (2) captures the nonlinear effect of a productivity increase in industry k on aggregate productivity. Mathematically, this nonlinear effect is determined by the *change* of Domar weight λ_k with respect to the change in productivity. Baqee and Farhi (2020) show that this nonlinear effect can be sizable for industries that are strong complements to the economy, such as oil. Equation (2) also implies that the Domar weight λ_k, and its change $d\lambda_k/d(\log A_k)$ are sufficient statistics for estimating the aggregate productivity gain, up to the second-order approximation.

11. **Staff's estimates show that substituting all coal-based generators with solar and wind could boost the long-term GDP level by at least 1 percent.** The gross output-to-GDP ratio of the electricity generation industry was 2.9 percent during 2011-20. Applying (1), a 28 percent productivity increase in the electricity generation industry would lead to an increase in aggregate productivity by 0.8 percent (calculated as 28 percent times 2.9 percent). This estimate includes the direct and indirect effects through electricity generation industries and all other upstream and downstream industries up to the first-order approximation. The nonlinear effect on aggregate productivity, captured by the second-order term -½ [dλ/d(log A)]*dlog(A) in (2), is likely small for a productivity increase in the electricity generation industry. The rationale is that the electricity generation industry's gross-output-to-GDP ratios were stable during 2011-20 (text chart), implying that electricity generation has close-to-unit elasticity of substitution (that is, neither a strong complement nor strong substitute to the economy) when the costs of electricity are on a declining path as observed during 2011-20. Because the underlying estimation methodology described in Box 1 implicitly assumes that the total sizes of productive factors (capital and labor) are fixed, a "capital multiplier" should be added to reflect that the economy-wide capital stock will increase as a result of the aggregate productivity increase. Assuming a standard capital share of one third, this capital multiplier is approximately 1.5 (calculated as 1/(1-1/3) = 1.5). The 0.8 percentage point increase in aggregate productivity thus translates into a 1.2 percentage point increase in GDP.[4]

Chile: Gross Output of Electricity Generation

(In percent of GDP)



Sources: BCCh and IMF staff calculations.

12. **The estimated long-term GDP gain is likely a lower bound because it is based on existing technology.** The estimated GDP gain is entirely driven by the productivity increase in electricity generation from the change of energy composition and the spillover to other industries through the existing input-output relationships. Our estimate assumes away the possible future technological changes that could either directly increase the productivity of renewable energy generation (e.g., a further decline in solar panel installation costs) or strengthen the influence of electricity on the rest of the economy. For example, a technological breakthrough that lowers the production and transportation costs of green hydrogen could result in a stronger linkage between the chemical industry (and its downstream industries) and the electricity generation industry. The

[4] This "capital multiplier" is illustrated in Jones (2011). As an example, suppose real output Y=AKaL1-a where A is the productivity level and a=1/3 is the capital share. Capital stock follows K'=sY-δK where s and δ are investment and depreciation rates. For any given A, the steady-state output level is Y=A1/(1-a)(s/δ)aL. That means, a one-percent increase in A will result in a 1/(1-a) percentage points increase in Y.

larger influence of the electricity generation (i.e., a larger λ) could amplify the impact of a productivity increase in electricity generation on aggregate GDP[5].

13. Compared to other studies, the moderate estimated long-term GDP gain is also driven by two other factors. First, the estimate of the GDP gain is a "net" gain instead of a "gross" gain. It assumes that the output increase from the increase in the production scale of one industry (e.g., electricity) may be partially offset by the decline in the production scales of some other industries, as they are competing for production resources (e.g., engineers). This "net" approach is different from GIZ and Hinicio Chile (2020) which estimate the gross gain in employment or value-added in a partial equilibrium framework, without considering that the same engineer who moves to renewable energy industries can no longer work in the manufacturing sector. Second, the estimate of the long-term GDP gain refers to the permanent increase in the steady-state GDP level as a result of the changes to the energy composition in electricity generation. This differs from the estimates of aggregate gain in some other studies that also count the temporary gains during the transition path. For example, GIZ and Hinicio Chile (2020) estimate that developing the green hydrogen industry in Chile will generate 255,000 jobs, but most of these jobs would be from the construction sector during the (temporary) construction phase.

14. Besides the long-term GDP gain, the expansion of renewable power would also increase the resilience of the economy to fossil fuel price shocks that tend to have nonlinear negative effect on the economy. The nonlinear effect captured by the last term of equation (2) can be asymmetric: while the nonlinear positive effect of electricity supply on the economy could be negligible when real electricity costs are on the decline (e.g., during 2011-20), a sizable rise in electricity generation cost could have a nontrivial nonlinear negative impact on GDP. The previous text chart shows that electricity generation's gross output-to-GDP ratio was 4.1 percent in 2008, significantly higher than the 2.9 percent average in 2011-20. This was due to the rise in the international coal prices (from USD 52 per tonne in 2006 to USD 138 per tonne in 2008) and the higher costs of importing natural gases from Argentina during 2005-08 (Serra 2022), both of which drove up the average costs of electricity generation. Because it is difficult to cut electricity demand within a short period of time, the rise in electricity prices led to higher values of electricity generation (despite somewhat lower quantities). Therefore, when there is a sizable cost increase to electricity generation (as observed in 2008), electricity becomes a complementary good to the rest of the economy that is hard to be substituted, causing a rise in its output-to-GDP ratio and a fall in

[5] There are also factors that could potentially overstate our estimate. In particular, our cost assumption is based on the levelized cost of electricity generation (LCOE) excluding transmission and storage costs. Because wind and solar power tend to have higher transmission and storage costs than fossil fuels, the assumed reduction in the unit costs of electricity based on the LCOE (which excludes transmission and storage costs), might be too high, though it is plausible that with technological progress transmission and storage costs will fall. A potential alternative would be to use the value-adjusted levelized cost of electricity generation (VALCOE) instead of the LCOE, as VALCOE takes into account the additional costs such as storage and interconnections. However, VACLOE is still a new concept and availability of estimates is limited.

aggregate GDP. The higher electricity cost (by about 38 percent compared to 2011-20 average) in 2008 is estimated to have lowered the GDP in 2008 by 1.3 percent.[6]

C. The Potential Role of State Support Policies

15. **Could it be economically efficient for the state to actively support industries related to the renewable energy sector?** Chile is a market economy with generally low levels of government intervention, but state support to certain industries exists, mainly through its development agency Corfo (Griffith-Jones et al., 2018). Related to the development of renewable energy, recent examples include the USD 1 billion financing support towards the development of green hydrogen as well as nonpecuniary legal or regulatory changes.[7] The cost-benefit analysis of state support policies, however, is often challenging for a few reasons. First, there is no unique standard for the types of "benefit" and "cost" to be considered. The comparisons can yield different outcomes, depending on whether the benefits of certain policies include output, employment, or carbon emission. Second, industries are interconnected. Subsidizing one industry would often have a consequential impact on other industries, complicating the analysis of net benefits.

16. **Liu (2019) develops a framework for comparing the economic costs and benefits of subsidizing certain industries in a production network.** Liu (2019) focuses on the "economic" benefits and costs while abstracting from the implications on health and emissions. In his framework, the government levies a lump sum tax to finance government consumption and industrial subsidies. Therefore, the tradeoff of higher subsidies is the increase in aggregate private consumption (due to the subsidies' net positive impact on aggregate output) versus the lower government consumption (due to higher subsidy expenditure).

17. **In this framework, the justifications for state support are the market imperfections that could distort the allocations of productive factors across industries.** In his setup, industries are interconnected through input-output relationships. Each industry has its market imperfections modeled as tax-equivalent wedges. These market imperfections can be in the form of market powers, taxes, or financial frictions, all of which would increase the costs of industry i to procure intermediate inputs from other industries. He shows that in equilibrium the negative effects of market imperfections in industry i could transmit to and accumulate along the value chain. As a result, industries that are at the upstream of a long value chain or have extensive input-output linkages with other high-imperfection industries tend to have high-than-efficient prices and lower-than-efficient production scales. There is room for the government to correct this inefficient allocation of labor and capital by subsidizing these industries.

18. **We apply the methodology in Liu (2019) to examine whether state support to industries related to renewable energy would have benefits larger than costs.** Operationally, Liu (2019) constructs a "distortion centrality" indicator f(i) for each industry i from the Input-Output

[6] This calculation follows that (2) can be approximated by ½*(λ+λ')*dlog(A) where λ and λ' are the Domar weights before and after the productivity shock: ½ * (4.1 percent + 2.9 percent) * 38 percent = 1.3 percent.

[7] Serra (2022) documents that a series of legal amendments in the 2010s "lowered entry barriers in generation".

table and separately estimates industrial-level market imperfections (Box 2). He shows that distortion centrality is a sufficient statistic for the benefit-to-cost ratio of increasing subsidies: it mathematically equals the marginal increase in private consumption divided by the marginal decrease in government consumption, as the result of higher subsidies. We apply this framework to calculate the distortion centrality by industry in Chile.

19. The 2019 Input-Output (IO) table compiled by the BCCh serves as data input for the production network. The 2019 IO table includes 111 industries. For each industry, the IO table includes the nominal values of its purchase of intermediate inputs from other industries and imports. Because Chile is an open economy, we constructed one industry called the "external trade" industry. The external trade industry purchases other industries' exports and is the supplier of imports of other industries and imports for final consumption.

20. Market imperfections are measured in two ways. The first approach is to calculate market imperfection parameters x(i,j) using industry j's operation surplus-to-gross output ratio based on the IO table for all 111 industries plus the added "external trade" industry variable.[8] The second approach is to use the "markup" measure in Benguria et al. (2023) for ten manufacturing sectors in Chile.[9] As discussed by Liu (2019), for China and Korea, the distortion centrality indexes calculated using different measures of market imperfection tend to be highly correlated.

Box 2. Liu (2019) on the Cost-Benefit Analysis of Industrial Policy

Liu (2019) develops a method to compare the economic benefits and costs of subsidizing industries in a production network.

Production network. There is one final consumption good and N types of intermediate goods. The production of the final consumption good requires intermediate goods as inputs: $Y = F(Y(1), Y(2), .., Y(N))$. For each intermediate good i, its production requires labor input $L(i)$ and other intermediate goods, using the technology $Q(i) = Fj(L(i), M(i,1), M(i,2), \dots M(i,N))$. Therefore, each intermediate good i can be used to produce other intermediate goods or the final consumption good, and its market clear condition is $Q(i) = Y(i) + \sum_{j=0}^{N} M(j,i)$. The markets for the final and intermediate goods are competitive, such that all production firms are price-takers. Households inelastically provide labor to production firms $L = \sum_{i=0}^{N} L(i)$. Households' consumption equals their after-tax wage income $C = wL - T$.

Market imperfections. For an intermediate good producer i, its purchase of input j incurs a deadweight loss $x(i,j)P(j)M(i,j)$, where $P(j)$ is the producer price of intermediate good j, and $x(i,j)$>0 is a wedge between the producer price and the purchaser price paid by producer i. Liu (2019) shows that this reduced-form deadweight loss can be micro-founded by financial frictions encountered by producer i (e.g., upfront payment to be financed by banks) or the producer's market power. The economy-wide GDP is defined as the total output of the economy netting the deadweight loss: GDP= $Y - \sum_{i=0}^{N}[\ \sum_{j=0}^{N} x(i,j)P(j)M(i,j)]$.

[8] While a caveat of this approach is in principle that capital income will be counted as market imperfections, this may be not a serious concern in practice if industries with high capital intensity are also the industries with high market imperfections due to their larger need for financing.

[9] For industries in the manufacturing sector, we impute the market imperfections with the estimates from Benguria et al. (2023). For other industries, we impute the values of market imperfections with the average cross-industry average market imperfections.

Box 2. Liu (2019) on the Cost-Benefit Analysis of Industrial Policy (Concluded)

Tax and industrial policy. The government collects a fixed amount of lump-sum tax T from households. This revenue is used to finance government consumption G and industrial subsidies. Industry subsidy is applied on the purchase of intermediate goods or labor, so that the effective cost for producer i to purchase goods j is $1 + x(i,j) - s(i,j)P(i,j)$, where $s(i,j)$ is the subsidy rate.

Cost-benefit comparison. Liu (2019) compares the benefits and costs of increasing subsidy rate $s(i,j)$. The marginal benefit of increasing the subsidy rate is characterized by the changes to total output and household consumption due to the cheaper effective intermediate input prices $dC/ds(i,j)$. The cost of increasing the subsidy is the reduction in government consumption to finance the higher subsidy $dG/ds(i,j)$, holding government revenue unchanged. The ratio between $d(C)/ds(i,j)$ and $dG/ds(i,j)$ captures the comparison of the benefits and costs of subsidies: if the ratio is larger than 1, the economy-wide benefit is larger than cost.

Distortion centrality. Liu (2019) constructs a "distortion centrality" indicator $f(i)$ for each industry i, which is defined as the ratio between industry i's "influence" $u(i)$ divided by the Domar weight $\gamma(i)$. The "influence" indicator measures $u(i)$ the impact of a productivity gain in industry i on aggregate GDP through the production network and is therefore a measure of the marginal economic benefit of increasing subsidies to industry i. The Domar weight $\gamma(i)$ measures the size of the industry and is hence an indicator of the marginal subsidy costs under a given subsidy rate. Therefore, $f(i)$ is a measure of the marginal benefit-to-marginal cost ratio of subsidizing industry i. Formally, Liu (2019) shows that

$$\frac{\left[\frac{d(C)}{ds(i,j)}\right]}{\left[-\frac{dG}{ds(i,j)}\right]} = f(i)$$

Thus, $f(i)$ is a **sufficient statistic** for the cost-benefit comparison of subsiding industry i: when $f(i)$ >1, the marginal benefit of increasing subsidy is higher than the marginal cost. The indicators $u(i)$, $\gamma(i)$ and $f(i)$ can be derived from the Input-Output (IO) table and estimated market imperfections by industry. He further shows that distortion centrality can also be calculated as the solutions to

$$f(j) = \alpha\theta(F,j) + \sum_{i=0}^{N} f(i) * [1 + x(i,j)] * \theta(i,j)$$

for all j=1, 2, ..., N.

Here α<1 is a constant, $\theta(F,j) = \frac{Y(j)}{Q(j)}$ and $\theta(i,j) = M(i,j)/Q(j)$ are the shares of output j used to produce final consumption good and intermediate good i, respectively. Intuitively, industries with higher distortion centrality are the industries that supply most of their outputs as intermediate inputs to other high-distortion centrality industries.

Results

21. **The text table lists the distortion centrality estimates of selected industries related to renewable power.** Column A is the baseline specification, which incorporates international trade by adding an external trade industry that purchases exports from (and supplies imports to) other industries. The market imperfection parameter x(i,j) is proxied by industry i's operating surplus-to-gross output ratio. In Column B, the market imperfection parameter x(i,j) is taken from Benguria et al. (2023). Columns C and D report the distortion centrality estimates in a closed economy setup (excluding the constructed "external trade" industry) by treating exports as final consumption. In

general, for exporting industries (e.g., furniture), the estimates of f(i) under the two "open economy" specifications are higher than under the "closed economy" specifications. The reason is that export income could be an important FX source to finance other industries' intermediate input imports, strengthening the influence of these exporting industries in the production network.

22. **The analysis indicates that the benefits of having targeted support for the transmission of electricity exceed costs.** The estimates in Column A show that if the government increased the subsidies to the electricity transmission industry, the increase in total private consumption could be 1.5 times the subsidy expenditure. The reason electricity transmission has a high subsidy benefit-to-cost ratio lies in the production structure: electricity transmission is upstream of electricity generation, and both industries are critical suppliers of almost all other industries. As shown in Columns C and D, the estimated benefit-to-cost ratios of supporting the electricity transmission industry are even larger in a closed economy setting. The critical role of electricity transmission is also emphasized in Gonzales et al. (2023) who analyzed the catalytic role of the SING-SIG transmission line projects.

Chile: Estimated Distortion Centrality f(i) for Selected Industries

Industry	Open Economy		Closed Economy		Output-to-GDP
	A 1/	B 2/	C 1/	D 2/	(Domar weight)
Transmission of electricity	1.50	1.33	1.95	1.80	0.4%
Maritime transport	1.33	1.44	1.53	1.58	0.4%
Manufacture of basic chemicals	1.31	1.33	0.85	0.85	1.6%
Gas and steam supply	1.30	1.25	1.92	1.89	0.6%
Manufacture of other chemical products	1.30	1.27	0.96	0.95	0.5%
Electricity generation	1.29	1.22	1.20	1.15	2.9%
Electricity distribution	1.01	0.97	1.21	1.17	0.6%
...					
Manufacture of furniture	0.70	0.68	0.34	0.32	0.4%

Source: BCCh and IMF staff calculations.

1/ Reports the estimates of f(i) based on industry-level markup proxied by operating surplus-to-output ratios in an open (closed) economy setting.

2/ Reports the estimates of f(i) based on sector-level markup estimated by Benguria et al. (2023).

23. **The estimated subsidy benefit-to-cost ratios of a few other related industries are also larger than one.** These industries include maritime transport and manufacture of chemicals (which include the transportation and production of green hydrogen and its derivatives), gas, and steam supply (which is upstream of electricity generation). On the contrary, industries close to final consumption, such as the manufacture of furniture shown in the table, tend to have benefits of subsidy smaller than costs.

24. **The results of the analysis have a few caveats.** First, the "benefits" and "costs" considered in this analysis are the solely the estimated increase in total output (or consumption) against subsidy expenditure. Some important social and environmental benefits or costs, such as health and carbon emissions, are not considered in this analysis. Second, the type of inefficiency that can justify the need for government intervention in this framework is the inefficient distribution of productive factors across industries. There could be other reasons, such as externalities from technological diffusion, which could also justify the rationale for state support.

References

Baqaee, David and Emmanuel Farhi (2019) "The Macroeconomic Impact of Microeconomic Shocks: Beyond Hulten's Theorem," Econometrica, vol. 87(4), Pages 1155-1203.

Benguria, Felipe, Alvaro Garcia-Marin and Tim Schmidt-Eisenlohr (2023) "Trade Credit and Relationships." CESifo Working Paper 7600.

Feldman, David, Vigesh Ramasamy, Ran Fu, Ashwin Ramdas, Jal Desai, and Robert Margolis (2020) U.S. Solar Photovoltaic System and Energy Storage Cost Benchmark: Q1 2020.

GIZ and Hinicio Chile (2020) "Cuantificación del Encadenamiento Industrial y Laboral para el Desarrollo del Hidrógeno en Chile."

Gonzales, Luis, Koichiro Ito and Mar Reguat (2023) "The Investment Effects of Market Integration: Evidence From Renewable Energy Expansion In Chile." Econometrica, Vol 91, No. 5, Page 1659-1693.

Griffith-Jones, Stephany, Maria Luz Martinez Sola and Javiera Petersen Muga (2018) "The Role of CORFO in Chile's Development: Achievements and Challenges." The Future of National Development Banks. Oxford University Press.

Hulten, Charles (1978) "Growth Accounting with Intermediate Inputs." The Review of Economic Studies, Vol. 45, Issue 3, Page 511-518.

International Energy Agency (2020) Projected Costs of Generating Electricity.

Jones, Charles (2011) "Intermediate Goods and Weak Links in the Theory of Economic Development", American Economic Journal: Macroeconomics, Vol. 3, No.2, Page 1-28.

Liu, Ernest (2019) "Industrial Policies in Production Networks." The Quarterly Journal of Economics, 1883-1948.

Ministry of Energy (2020) Chile, Green Hydrogen, an Energy Source for a Zero Emission Planet.

OECD (2021) Economic Policy Reforms 2021: Going for Growth—Chile.

REN 21 (2022) Renewables 2022 Global Status Report Chile Factsheet.

Serra, Pablo (2022) "Chile's Electricity Markets: Four Decades on From Their Original Design." Energy Strategy Reviews 39 100798.

Zissler, Romain (2020) Innovative Decarbonization Policies: Chile.

CYBERSECURITY AND FINANCIAL STABILITY: CONSIDERATIONS FOR CHILE[1]

In recent years, the Chilean financial sector experienced a series of cyberattacks, and this growing global risk of cybersecurity is posing a threat to the sector. Banks and financial market infrastructures appear to be resilient against cybersecurity risks, supported by a comprehensive regulatory framework, but lack of substitutability and high concentration of these institutions could pose systemic risk to the financial system. Moreover, given the current business segment of the Chilean fintech sector, expansion of the sector would lead to larger exposures to cybersecurity risk which the ongoing regulation of the sector by the authorities aims to mitigate. Ensuring sufficient human resources to ensure effective cybersecurity supervision of the financial sector as well as implementing ongoing policy initiatives, are warranted.

A. Introduction

1. **Cybersecurity risks have been growing globally and Chile's financial sector already suffered from several cyberattacks.** As the economy and financial sectors have become more digitalized and interconnected, the risks associated with cyberattacks are escalating. The number of cyberattacks (malicious use of IT technologies) in OECD peers increased dramatically over the past decade, especially since 2020 (Figure 1), according to University of Maryland CISSM Cyber Attacks Database (Harry and Gallagher, 2018).[2] Notably, the share of cyberattacks on the financial sector ('finance and insurance sector' in the following chart) was higher in Chile than in regional and OECD peers. The motives of attacks are mainly financial and cross-border cyberattacks are not rare.

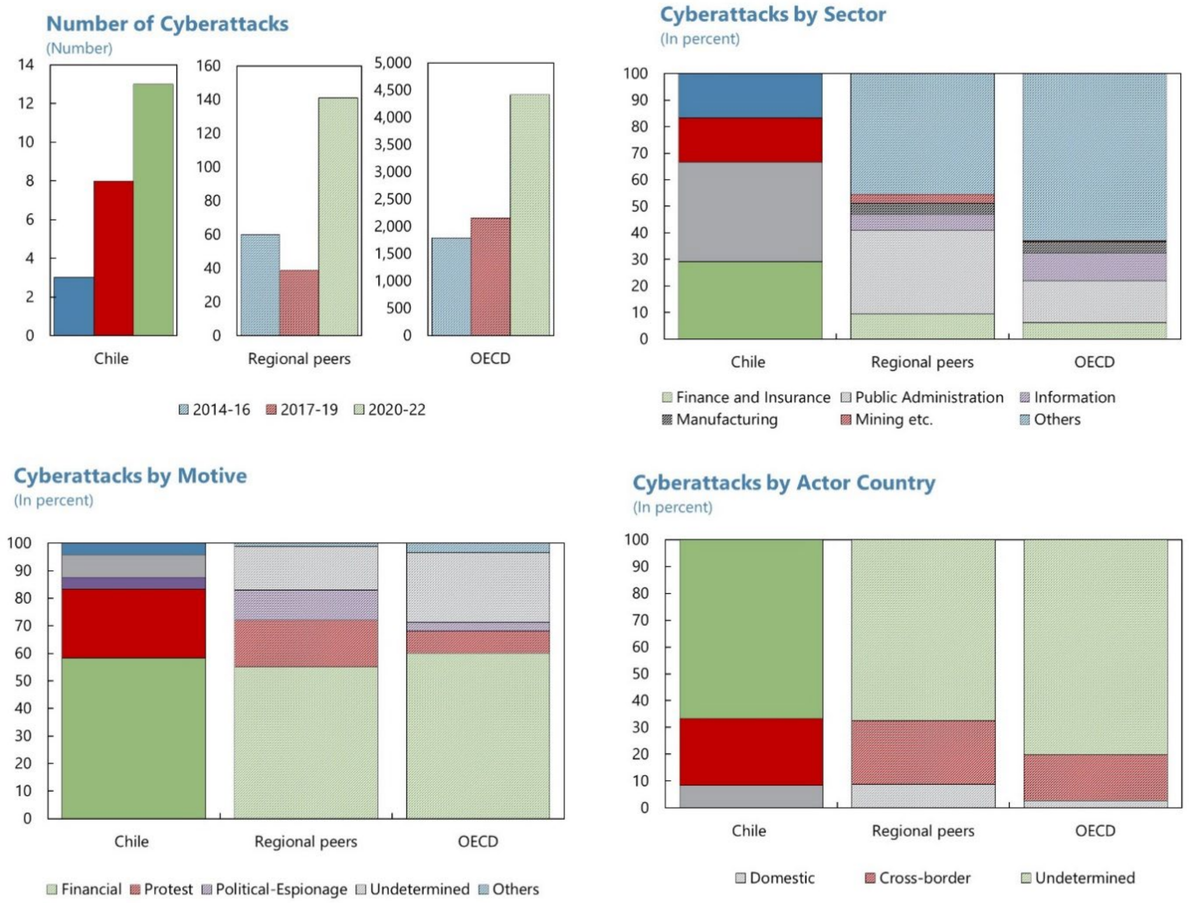
2. **The increasing cybersecurity risk is posing a threat to Chile's financial sector, as it is in most other financial systems.** While past cyberattacks did not cause systemic financial instability, they can pose stability risks going forward. For instance, a cyberattack on critical financial operations could erode confidence, leading to reluctance in extending liquidity or credit, potentially causing deposit runs (Duffie and Younger, 2019) and interbank payment failures (Eisenbach et al., 2022). Disrupting specific institutions' critical services could also disrupt massive financial transactions due to low substitutability (Healey et al., 2018). These risks are amplified by interconnected financial linkages and technology dependencies, including exposure to third-party IT service providers (Adelmann et al., 2020).

[1] Prepared by Tatsushi Okuda. The paper has benefited from the synergies and association with the ongoing work for the IMF's Global Financial Stability Report. The author would like to thank the BCCh and CMF staff for the helpful discussions.

[2] This database is prepared by leveraging an application to scrape data from relevant cyber sources, which is then reviewed and coded by the research team. Note that this database covers only the incidents that had media coverage, and many of those which were blocked by the targets are not included. Indeed, according to Trend Micro, in Chile, the number of malware detections, email threat detections, and malicious URL detections in the first half of 2021 were, respectively, over 2 million, 47 million, and 1 million, which were much larger than the number of incidents reported by this database.

3. **The CMF and the BCCh consider cybersecurity risk a material risk, consistent with the international debate.** In the global context, cybersecurity risk is recognized as a top concern by regulators and central banks (FSB, 2017a; FRB, 2021; ESRB, 2020; FSOC, 2022; ECB, 2022; BIS, 2022a).[3] The Chilean authorities have also heightened their attention to this risk. The Financial Market Commission (CMF) included cybersecurity risk in its 2022 strategic plan and the Central Bank of Chile (BCCh)'s Financial Stability Reports (FSRs) have addressed cyber risk since 2016, including a thematic box on 'Cyber Security and Financial Stability' in the 2018 FSR.

Figure 1. Selected Economies: Cyberattacks



Sources: University of Maryland CISSM Cyber Attacks Database and IMF staff calculations.

Note: "Mining etc." includes Mining, Quarrying, and Oil and Gas Extraction. "Regional peers" indicates the sum of Brazil, Mexico, Colombia, Argentina, and Peru. "OECD" indicates the sum of OECD countries.

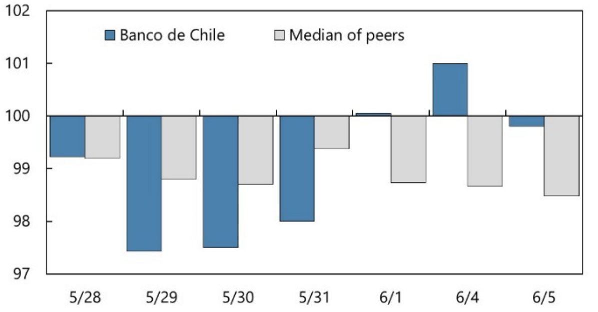
[3] The IMF assessed cybersecurity risk in several Financial Sector Assessment Programs (FSAP) (Switzerland in 2019; Belize and Norway in 2020; Mexico, South Africa, and the United Kingdom in 2022; Iceland and Sweden in 2023) and provided Technical Assistance (e.g., Trinidad and Tobago in 2023).

B. Cyberattacks on the Chilean Financial Sector

4. Past cyberattacks on the Chilean financial sectors were concentrated on banks.[4] Notably, the Chilean banking sector encountered cyberattacks that affected a few large banks which are currently designated as the Domestic Systemically Important Banks (D-SIBs).[5] Specifically, Banco de Chile and Banco de Estado experienced attacks in 2018 and 2020, respectively (Box 1). In terms of the cyberattacks on Banco de Chile, the bank's equity price declined following the disclosure of the cyberattacks (on May 28, 2018).[6] Furthermore, in 2019, a cyberattack targeted Redbanc, the critical third-party IT service provider of ATMs and other services on retail payments.[7]

Chile: Bank Equity Prices

(Open price on May 28, 2018=100)



Sources: Santiago Stock Exchange and IMF staff calculations.
Note: Close prices on each day. "Peers" includes Banco de Crédito e Inversiones, Banco Santander-Chile, and Banco Itaú Chile.

C. Cybersecurity Risk for Banks

5. Rapid digitalization has increased Chilean banks' exposures to cybersecurity. Since 2013, the number of Chilean banks' branches has decreased by around 35 percent, and the number of online banking accounts has significantly increased by more than four times,[8] reflecting Chilean banks' efforts to transition to digitalized financial activities (Figure 2). In line with the developments, their IT expenses (e.g., IT and communication expenses and outsourcing services for data processing) have been rapidly increasing.[9] While this enables banks to improve efficiency of their business operations and enhance their business opportunities, it also increases banks' exposures to cybersecurity risk.

[4] Information and data are from the University of Maryland CISSM Cyber Attacks Database and the BCCh's FSRs.

[5] D-SIBs are designated annually using a methodology developed by the CMF, based on the one from the Basel Committee and with the favorable agreement of the BCCh. The current D-SIBs were designated in March 2023.

[6] This observation is consistent with the empirical literature which documents that cybersecurity risk is priced in equity markets (Jamilov et al., 2021; Florackis et al., 2023).

[7] Moreover, the CMF experienced cyberattacks in March 2021 while these attacks did not disrupt the CMF's platforms or services, as the organization promptly activated cybersecurity protocols and containment measures to ensure the continuity of services.

[8] During the pandemic, the number of online bank accounts was boosted as these accounts were used for the transfer of state aid to lower-income households and due to the greater use of online purchases. This shift led banks to expand their digital offerings and close offices. The rise of online bank accounts may also partially reflect Banco Estado's introduction of Cuenta RUT in 2006 which is a demand account featuring simplified opening procedures, no income prerequisites, and no maintenance fees.

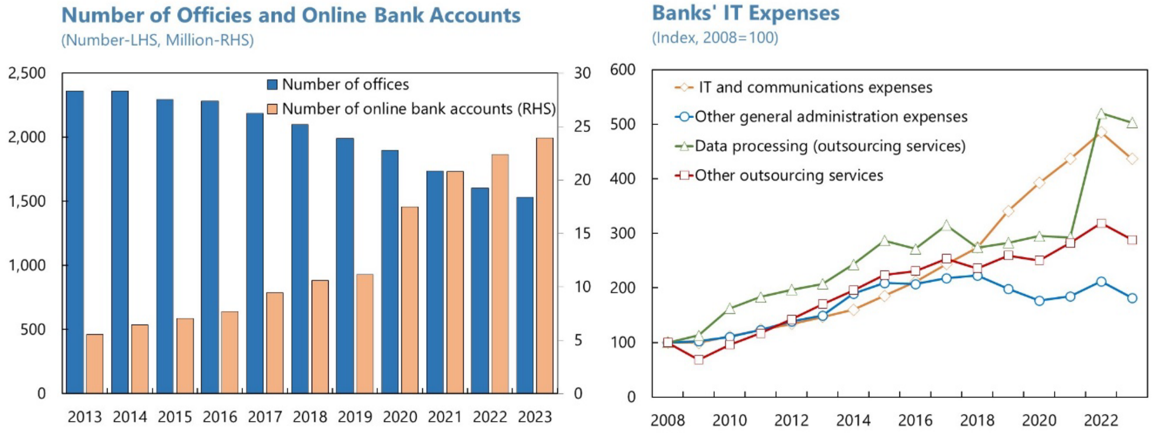
[9] The growth rate of Chilean banks' nominal IT expenses in the 2010s (threefold) is similar to that of U.S. banks (Modi et al., 2022; He et al., 2023). Because the inflation rate has been moderately higher in Chile than in the U.S., the growth rate of real IT expenses may be modestly higher in the U.S. than in Chile.

Box 1. Cyberattacks on the Chilean Banking Sector

Banco de Chile (2018)	On May 24, 2018, Banco de Chile suffered a major cyberattack that infiltrated a significant portion of its 9,000 computers and 500 servers. This virus rendered them non-rebootable by wiping their hard drives. To safeguard consumer accounts, the bank disconnected 9,000 workstations, causing the suspension of operations at nearly 400 branches nationwide for about two weeks. During this period, hackers quietly exploited the SWIFT bank messaging service for fraudulent transactions, resulting in approximately US$10 million being transferred abroad, specifically to Hong Kong.
Banco Consorcio (2018)	On November 6, 2018, Banco Consorcio fell victim to a cyberattack that led to a loss of just under US$2 million. The bank reported that cybercriminals had tampered with its international transfer procedures, creating unauthorized charges within an account held by the bank at a correspondent institution located abroad. The bank also reported that the financial loss was covered by insurance, and the incident had no adverse effects on client data or the bank's operational systems.
Redbanc (2019)	On January 15, 2019, Redbanc, the entity responsible for the technical operation of the entire ATM network in the country, suffered a cyberattack. The breach occurred when a Redbanc employee came across a job advertisement on a business and employment-focused social media platform and subsequently participated in a virtual interview. During the interview, the attackers convinced the employee to download malicious software onto their system, thereby granting the attackers access to Redbanc's network. Redbanc reported that its day-to-day business operations were not disrupted by this cyberattack.
Banco Estado (2020)	On September 6, 2020, Banco Estado reported a ransomware attack on its premises. The virus infected the systems when an employee accidentally opened a malicious file that was believed to be planted by hackers via a backdoor. The attack was detected when employees were unable to access the files on September 5. After the bank's report on the attack to Chilean police, the Chilean government promptly issued a nationwide cybersecurity alert to the country's private sector. The bank shut down all its branches for an investigation on September 7 after the attack occurred. Due to the network segmentation techniques in place, the bank's website, banking portal, mobile apps, and ATMs were unaffected while internal servers and devices were inaccessible to the employees.

Sources: University of Maryland CISSM Cyber Attacks Database, FSRs, and media reports.

Figure 2. Digitalization of Chilean Banks

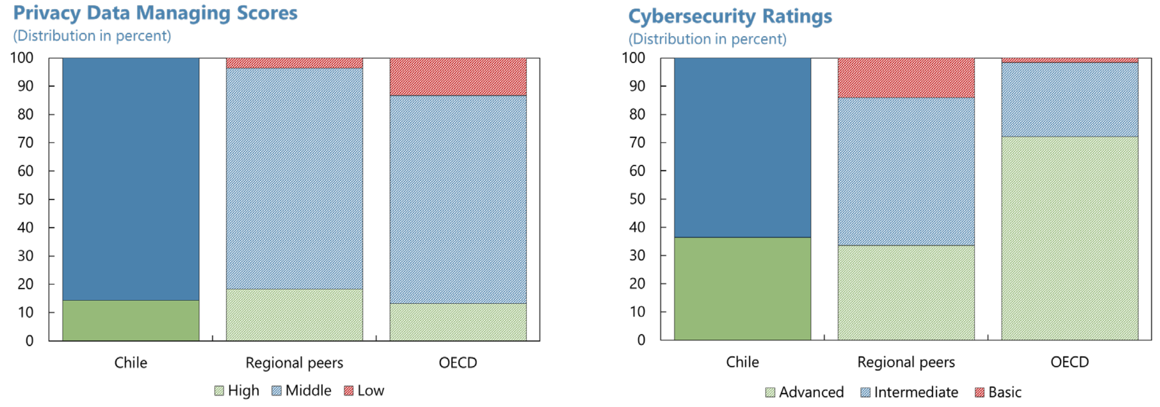


Sources: Financial Market Commission (CMF) and IMF staff calculations.
Notes: Number of offices in 2023 is as of September. Number of online bank accounts in 2023 is as of August. Expenses in 2023 are as of October 2023, annualized by multiplying 12/10.

Cybersecurity Levels

6. Chilean banks' cybersecurity levels appear slightly higher than regional peers while they seem to still lag behind OECD peers. Commonly used indicators show Chile to be better prepared to cybersecurity risk, compared with banking systems in the region reflecting that Chilean banks have intensified investment in cybersecurity[10] and established governance and measures to address cybersecurity risk (Figure 3).[11] However, compared with banks in OECD peers, Chilean banks may fall behind to some extent. The measures include a privacy data management score,[12] which is a proxy for the level of cybersecurity regarding data security, and the cybersecurity rating,[13] which roughly represents the unconditional probability of becoming victim of cyberattacks, considering both the likelihood of encountering cyberattacks and the likelihood of being affected by them. Both

Figure 3. Selected Economies: Cybersecurity Levels of Banking Sector



Privacy Data Managing Scores
(Distribution in percent)

Cybersecurity Ratings
(Distribution in percent)

Sources: Bitsight, MSCI, and IMF staff calculations.
Notes: In the left chart, "Low" indicates 0-4, "middle" indicates 5-8, and "high" indicates 9-10. In the right chart, companies are rated on a scale of 250 to 900, and "Advanced", "Intermediate", and "Basic" corresponds to 740-900, 640-730, and 250-630,"repsectively. "Regional peers" indicates the sum of Brazil, Mexico, Colombia, Argentina, and Peru. "OECD" indicates the sum of OECD countries. Privacy data management scores are as of 2022 and cybersecurity ratings are as of November 2023.

[10] For example, in its 2022 annual report, Banco de Crédito e Inversiones reported that it invested US$ 80 million to cybersecurity. Aldasoro et al. (2022a) empirically document that the firms which invest more in information technology security tend to be more resilient to cyberattacks.

[11] According to their 2022 annual reports, Chilean banks have contingency plans for cybersecurity incidents and regularly conduct cybersecurity training for employees. They also adopt international standards for the best practices to address cybersecurity risk including ISO/IEC 27001 (information security management), National Institute of Standards and Technology (NIST) cybersecurity framework, and the Payment Card Industry Data Security Standard (PCI-DSS). Some banks hire cybersecurity specialists as executives, such as Chief Information Security Officers (CISOs).

[12] The indicator is calculated based on the quality and coverage of data protection policy, organizational structure, internal control, and privacy-enhancing technologies etc., and provided by MSCI.

[13] This indicator is calculated based on three types of vectors: i) security practices, ii) the presence of malware or unwanted software, and iii) employee activities, and provided by Bitsight. In its 2022 annual report, Banco Santander Chile explicitly commits to scoring 800 points in this measure.

indicators, the privacy data management score, and the cybersecurity rating, are slightly better than that of its regional peers while the cybersecurity ratings are lower than OECD peers.[14]

Resiliency to Solvency Risk

7. The banking sector's solvency risk from cyberattacks appears contained so far. Cyberattacks frequently result in direct costs, including expenses for repairing compromised systems, compensating for data breaches, fines,[15] and legal fees, and it is important to understand the quantitative impact of cyberattacks on banks' solvency. Among the seven categories of operations losses,[16] the share of 'external fraud,' which is most relevant to cyber losses, dominates (Figure 4).[17] Using historical annual operational losses from internal and external frauds as the proxy for historical annual cyber losses,[18] the impact of the losses on banks' profitability is ranged predominantly between 0-0.5 percent of equity. The impact was higher in a few banks, exceeding 2 percent, but remained overall modest. Consistent with these observations, the maximum impact of the losses on capital ratios for each bank was less than 10 bps in most cases, with losses potentially higher for some banks.[19] Even under a stress scenario in which banks suffer the historical maximum stress observed in the sector,[20] the impact would range between 20-80 bps in all cases. Finally, when comparing the maximum of the historical annual losses to the capital required for operational risk by each bank,[21] significant heterogeneity is evident across banks. Some banks would experience losses exceeding 20 percent of their capital to operational risk, but in all cases capital to operational risk would fully cover the gross losses. Adding the maximum impact of historical annual operational

[14] In terms of privacy data management scores, Chilean banks outperform their OECD peers; however, this may be indicative of sample selection bias, as samples from advanced economies encompass both large and small banks, whereas samples from emerging economies only include large banks. Regarding sample size, that of the cybersecurity rating is much larger than that of privacy data management scores.

[15] Bouveret (2018) estimates the potential aggregate costs of cyberattacks to range between 10 percent to 30 percent of banks' net income. While there exist indirect costs, such as reputational damage which can have serious, long-lasting financial impacts, the literature has not yet covered this cost as it is difficult to estimate.

[16] i) Internal fraud: misappropriation of assets, tax evasion, intentional mismarking of positions and bribery, ii) External fraud: theft of information, hacking damage, third-party theft and forgery, iii) Labor practices and business safety: discrimination, workers' compensation, employee health and safety, iv) Customers, products and business practices: market manipulation, antitrust, improper trade, product defects, fiduciary breaches and account churning, v) Damage to physical assets: natural disasters, terrorism and vandalism, vi) Business interruption and systems failures: utility disruptions, software failures and hardware failures, and vii) Execution, delivery and process management: data entry errors, accounting errors, failed mandatory reporting and negligent loss of client assets.

[17] This 'external fraud' includes self-induced fraud by customers.

[18] 'Internal fraud' is included to consider the possibility that employees caused cyber incidents.

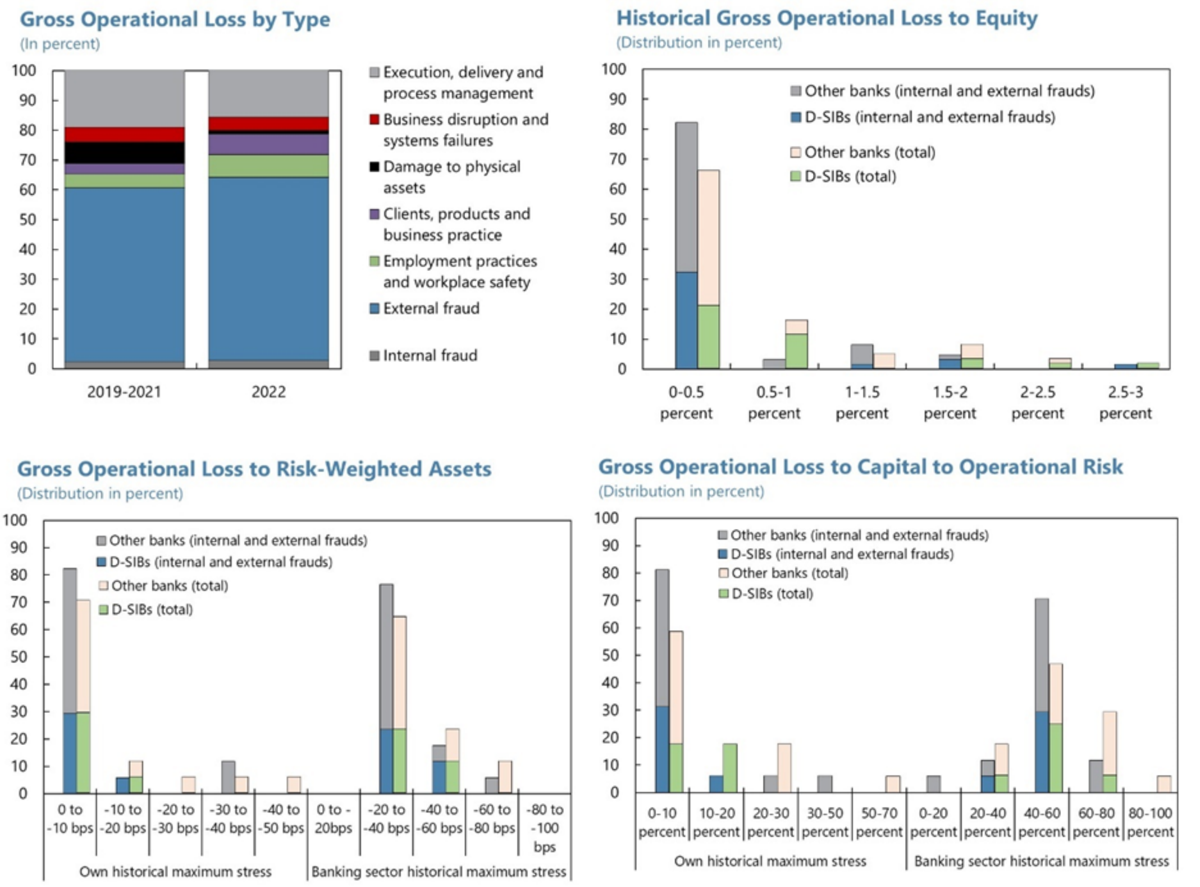
[19] The impact is calculated by dividing annual gross operational losses by risk-weighted assets.

[20] The maximum stress is calibrated to the maximum impact of historical operational losses to assets in the annual frequency panel dataset of all individual banks in 2019-22. The impact on capital ratios under the stress is calculated by multiplying the impact of historical operational losses on capital ratios by the ratio between maximum stress and historical impact in terms of operational losses to assets. The same applies to the calculation of the operational loss to capital to operational risk.

[21] The capital to operational risk is calculated by dividing the risk weighted assets for operational risk by 12.5, and the loss to capital ratio is calculated by dividing annual gross losses by the capitals to operational risk. Note that the share of risk-weighted assets for operational risk is around 10 percent among Chilean banks.

losses from incidents other than internal and external frauds increases the impacts, but the results remain broadly unchanged. Note that the calculations may overestimate the impact of cyber losses since data specifically related to operational losses from cyberattacks in Chile are unavailable, and the analysis uses bank-by-bank data on operational losses from internal and external frauds instead.[22]

Figure 4. Solvency Risk of Chilean Banks



Gross Operational Loss by Type
(In percent)

Historical Gross Operational Loss to Equity
(Distribution in percent)

Gross Operational Loss to Risk-Weighted Assets
(Distribution in percent)

Gross Operational Loss to Capital to Operational Risk
(Distribution in percent)

Sources: Financial Market Commission (CMF) and IMF staff calculations.

Note: "Historical Gross Operational Loss to Equity" indicates historical distribution of the impact of operational losses on equity in 2019-2022 and across all banks (62 samples, annual basis). In the bottom charts, "own historical maximum stress" on capital in 2019-2022 (annual basis). "Banking sector historical maximum stress" for internal and external frauds is calibrated based on the maximum impacts of historical losses from these frauds on total assets in 2019-2022 (annual basis) across all banks, and that for total is calculated by adding impacts of own historical maximum losses from other incidents on risk-weighted assets. Risk-weighted assets in 2021 are assigned to 2019 and 2020.

[22] The database is also expected to include the operational losses from the cyberattacks which were not reported in the media and thus are not included in CISSM Cyber Attacks Database. Aldasoro et al. (2020b) reported that while operational losses from cyber incidents represent a small fraction of total operational losses, they can significantly impact the total operational value-at-risk. Cohen et al. (2019) also suggest that cyber loss data shares a risk profile similar to non-cyber operational losses. This allows for the application of existing operational risk modeling techniques to assess the financial impact of cyber risk.

Resiliency to Liquidity Risk

8. Cyberattacks are considered a potential threat that could undermine bank liquidity. The literature highlights the importance of managing liquidity risk in the context of cybersecurity. Duffie and Younger (2019) argue that while capital adequacy ratios address operational risk, liquidity coverage ratios (LCRs) do not consider the liquidity risk associated with 'cyber runs,' which are serious and contagious bank runs caused by cyberattacks. The risks of such runs are heightened for banks that are heavily dependent on wholesale unsecured deposits. This is because unaffected large institutional depositors may swiftly withdraw their deposits as a precautionary measure.

9. Chilean banks appear resilient to the cyber-related liquidity risk, i.e., massive withdrawal of the uninsured wholesale deposits. Scenario assessments of LCRs, which is already introduced in Chile as a part of Basel III liquidity requirement, are used to assesses the resilience of Chilean banks' liquidity in response to 'cyber runs' above. Specifically, following Duffie and Younger (2019), two scenarios are considered: an 'adverse cyber scenario' and a 'severe cyber scenario,' assuming respective outflows of 50 and 75 percent from unsecured wholesale deposits (i.e., operational deposits and non-operational deposits in unsecured wholesale funding) due to massive deposit withdrawals by institutional depositors.[23] The analysis finds that most banks including all D-SIBs could meet a 100 percent LCR regulatory requirement in case of a large outflow of uninsured wholesale deposit due to cyberattacks (Figure 5).[24] The results reveal that Chilean banks are generally robust to such risks. Chilean banks' substantial holdings of high-quality liquid assets (HQLAs) partly contribute to this result, and more importantly, outflow rate assumptions for unsecured wholesale deposits to calculate the LCRs are the major source of the resilience.[25]

10. Chilean banks also appear robust to liquidity outflows from retail deposits. A few countries experienced bank runs triggered by the spread of the rumors via digital media (Bouveret, 2018; BOE, 2018; Duffie and Younger, 2019). When calibrating a scenario of 'retail deposit run' based on a Bulgarian bank run in 2014 (10 percent) in addition to 'severe cyber run scenario' for unsecured wholesale deposits,[26] the calculations suggest that most Chilean banks could withstand such a sizeable outflow (based on balance sheet data as of September-2023) due to the same reasons above while outflow rates for retail deposit are similar to their regional and OECD peers. It should be noted that the resilience may have been facilitated by the legacy of the temporary liquidity measures (Facility of Credit Conditional on Lending, FCIC) introduced by the BCCh during the

[23] The outflows from unsecured wholesale deposits are assumed to decrease high-quality liquid assets (HQLAs) by forcing banks to sell them. The outflows are also assumed to reduce their unweighted exposures to the deposits. The former channel decreases the LCRs while the latter channel increases the LCRs. Outflow rates for the deposits are assumed to remain unchanged.

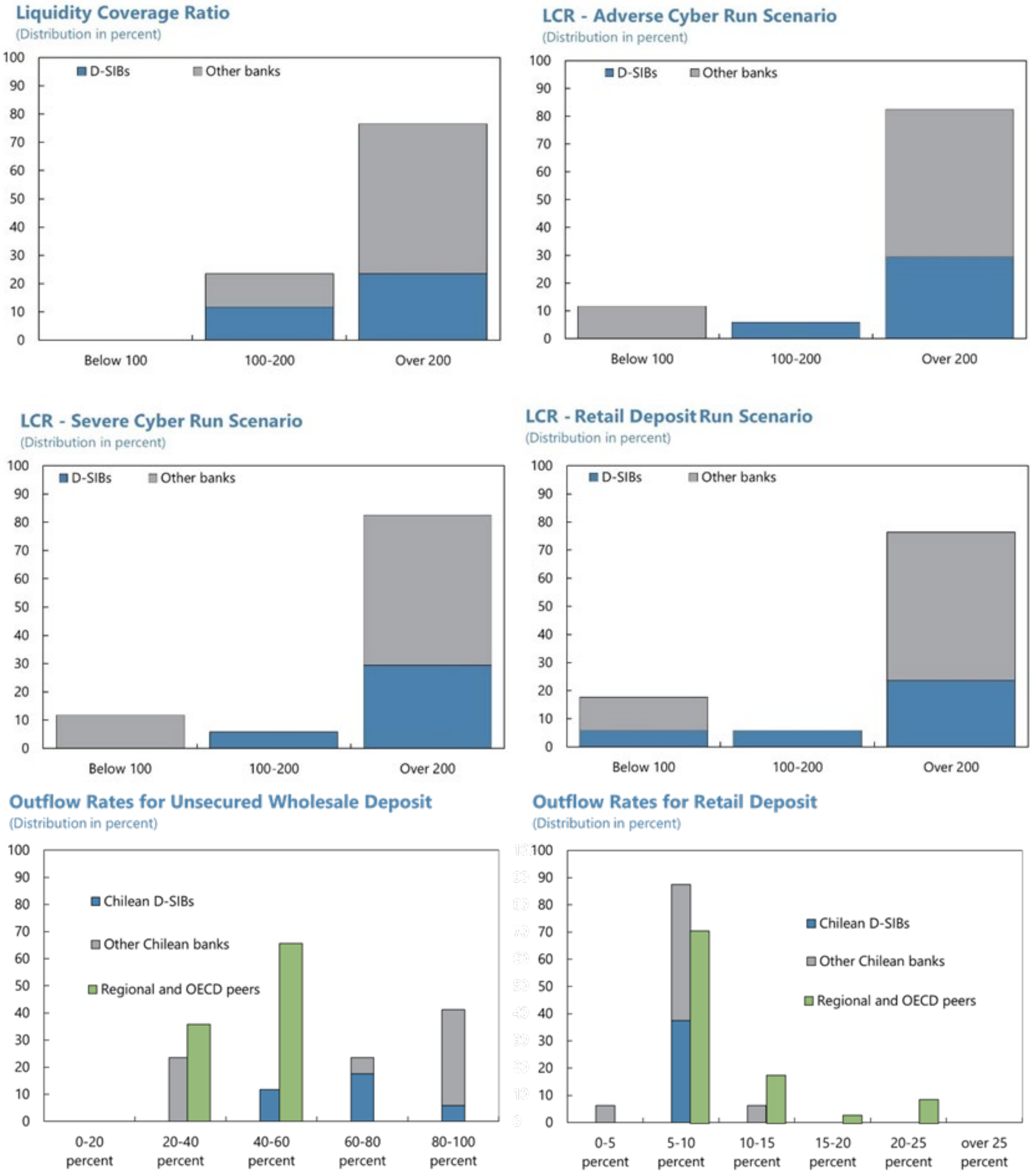
[24] Cyberattacks often occur during financial stress (Eisenbach et al. 2023) and thus, banks should continue to satisfy the 100 percent LCR requirement after cyberattacks.

[25] Note that the LCRs decrease to some extent if same outflow rates from secured wholesale funding are additionally assumed because the outflow rate assumptions for the item are low. However, the results remain overall unchanged.

[26] On June 27, 2014, Bulgaria's largest domestic bank, First Investment Bank (FIB), experienced a 10 percent deposit run due to false emails and social media rumors about a liquidity shortage, prompting the bank to use a government-provided liquidity assistance scheme.

pandemic, allowing banks to use their credit portfolios as collateral and potentially avoid the need to sell their HQLAs.[27] Moreover, due to the high interconnectedness within the financial system, the liquidity risk of individual banks may pose large externalities to the system. Thus, the authorities' close monitoring of this type of risk is warranted, and they should stand ready to provide liquidity to the system.

Figure 5. Liquidity Risk of Chilean Banks



Liquidity Coverage Ratio
(Distribution in percent)

LCR - Adverse Cyber Run Scenario
(Distribution in percent)

LCR - Severe Cyber Run Scenario
(Distribution in percent)

LCR - Retail Deposit Run Scenario
(Distribution in percent)

Outflow Rates for Unsecured Wholesale Deposit
(Distribution in percent)

Outflow Rates for Retail Deposit
(Distribution in percent)

Sources: Banks' Pillar III disclosures and IMF staff calculations.
Note: Liquidity Coverage Ratios are as of September 2023. The bottom charts indicate weighted average of the outflow rates of each item in unsecured wholesale deposit and retail deposit. "Regional and OECD peers" indicates D-SIBs in Brazil and Mexico, and G-SIBs in OECD countries.

[27] However, it should also be noted that the implemented Basel III liquidity requirement provides incentives for banks to continue holding HQLAs to meet a 100 percent LCR regulatory requirement, even after the unwinding of the FCIC.

Systemic Vulnerability

11. **Consistent with its regional and OECD peers, the Chilean banking sector is highly concentrated, which poses a risk of near-single points of failure in the financial system.** The three largest Chilean banks account for around 50 percent and the five largest banks for about 80 percent of total bank assets (Figure 6).[28] The literature underscores that a highly concentrated banking sector can result in near-single points of failure due to limited substitutability of financial activities (Brando et al., 2022).

12. **Third-party IT supplier risk is relevant for Chilean banks.** According to the literature, banks using third-party IT service providers face added cybersecurity risks. Attacks on these providers could infiltrate banks' systems, regardless of the banks' own cybersecurity measures (BIS, 2018).[29] Cyberattacks on IT suppliers can also create systemic risks, as they often result in their customers becoming simultaneous new victims (Crosignani et al., 2023). In Chile, the cybersecurity rating of IT service sectors is modestly higher than regional peers (and banks), implying that the cyberattacks on their third-party supplier risk may be relatively more contained. This might reflect the fact that Chilean banks have implemented the mitigation measures for the risk.[30] However, based on Capital IQ Pro supply-chain data,[31] although coverage is limited, three of the eight IT suppliers serving the Chilean banking sector provide services to multiple Chilean banks, indicating a systemic nature of third-party IT supplier risk in Chile.[32]

D. Cybersecurity Risk for Financial Market Infrastructures

13. **Financial market infrastructures (FMIs)[33] are considered critical entities in the context of cybersecurity risk.** FMIs could increase the financial system's vulnerability to cyber shocks due to low substitutability and high market concentration (BIS, 2014). For instance, if banks were compelled

[28] 17 banks are operating in Chile, in which six are D-SIBs (Banco de Chile, Banco de Crédito e Inversiones, Banco del Estado de Chile, Banco Santander-Chile, Banco Itaú Chile, and Scotiabank Chile) as of March 2023, accounting for around 90 percent of bank assets.

[29] For example, on June 27, 2017, Ukrainian banks and companies fell victim to a cyberattack by Russian hackers using the NotPetya virus. This malware spread rapidly through a software update for accounting programs, affecting a wide range of businesses, financial institutions, and government agencies. According to the National Bank of Ukraine's December 2017 Financial Stability Report, the attack impacted 35 percent of the Ukrainian banking sector by net assets and 32 percent by household deposits, with most banks facing operational difficulties for several days. Foreign multinational companies were also affected through their Ukrainian subsidiaries (Crosignani et al., 2023).

[30] According to their 2022 annual reports, Chilean banks have implemented measures to mitigate the cybersecurity risk from third-party IT suppliers such as setting cybersecurity standards for suppliers.

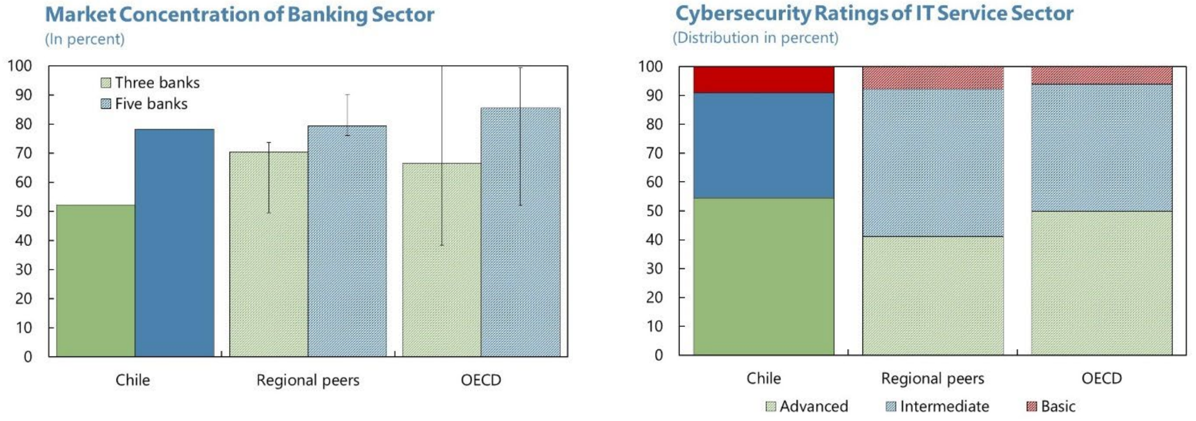
[31] The database is prepared based on banks' publicly disclosed data.

[32] On October 23, 2023, a Chilean telecommunications company, GTD, suffered a ransomware attack that affected part of its Infrastructure as a service (laaS) platform, disrupting online services. According to the media, about 3,500 firms were impacted by this incident. This incident highlights the importance of the third-party IT supplier risk in Chile. Moreover, in terms of the concentration of IT service providers, cloud computing services are reported to be highly concentrated globally (Carney, 2019).

[33] Payment systems (PS), central securities depositories (CSD), securities settlement systems (SSS), central counterparties (CCP) and trade repositories (TR) are designated as FMIs (BIS, 2012).

to redirect their payments without the netting and payment efficiencies from the cyber-attacked payment systems, it would necessitate additional liquidity for these payments, thus resulting in disruptions to market volumes and sudden price fluctuations (Brando et al., 2022). Against this backdrop, guidance, and best practices to address the FMIs' cybersecurity risk has been proposed.[34]

Figure 6. Selected Economies: Systemic Vulnerability of Chilean Banks



Sources: Bitsight, World Bank, and IMF staff calculations.
Notes: The left chart indicates assets of the top banks as a share of total commercial banking assets in 2021. The bars and whiskers of "Regional peers" and "OECD" indicate the median and max/min range of regional peers and OECD countries, respectively. In the right chart, "Computer Systems Design and Related Services" (NAICS code, 5415) is defined as IT service sector. "Regional peers" indicates the sum of Brazil, Mexico, Colombia, Argentina, and Peru. "OECD" indicates the sum of OECD countries.

14. In Chile, the risk from lack of substitutability is high. Six FMIs,[35] four of them private entities, operate as monopolies within their respective segments.[36] The Chilean high-value interbank payment systems (PSs) consist of Sistema LBTR, the central-bank operated real-time gross settlement system, complemented by ComBanc, a privately-owned net clearing system (Figure 7). DCV serves as the central security depository (CSD) for government and corporate securities, while

[34] For example, in 2016, the Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions published 'Guidance on cyber resilience for FMIs' (BIS, 2016), and in 2022 they published 'Implementation monitoring of the PFMI: Level 3 assessment on Financial Market Infrastructures' Cyber Resilience,' which summarized the adoption status of the guidance above in each country (BIS, 2022b). Additionally, one of the critical service providers in payment systems, the Society for Worldwide Interbank Financial Telecommunication (SWIFT), a global messaging network used by financial institutions to send and receive information is imposing SWIFT Customer Security Programme on users, to improve information sharing among SWIFT users, to increase the level of security awareness and education, and to establish a set of mandatory security controls that SWIFT customers must implement.

[35] Within the low-value payment system (involving credit cards, checks, and ATMs), CCA (Centro de Compensación Automatizado), a privately-owned for-profit corporation, operates alongside low-value clearinghouses. Moreover, implementation of Low Value Payment Clearing Houses (CPBV) is in progress; CCA will start to operate 'Clearinghouse for interbank Electronic Funds Transfers' at the end of 2023-early 2024, and the BCCh is currently reviewing internal rules of other six CPBVs.

[36] Moreover, according to the BCCh's FSR, the BCCh has promoted incorporating the Chilean peso into the Continuous Linked Settlement (CLS) in Switzerland, the world's leading provider of FX settlement services. If successful, integrating the LBTR system with interbank payment systems in other countries via CLS would heighten cybersecurity risks for Chilean financial sector while it also enhances the efficiency of financial activities.

CCLV operates as a securities settlement system (SSS) for debt securities and money market instruments. Two central counterparties (CCPs), ComDer and CCLV, hold monopolistic positions in their respective segments: ComDer covers over-the-counter (OTC) derivatives, while CCLV handles equities and exchange-traded derivatives. Additionally, the BBCh operates SIID-TR as trade repository (TR) for reporting foreign exchange derivatives transactions. Compared with regional peers, in Chile, PSs and CSD are relatively larger while CCPs are smaller.[37] Most of the participants in the PSs and ComDer (CCP) are banks, but DCV (CSD) and CCLV (CCP) have many other participants.

Chile: Financial Market Infrastructure

	Sistema LBTR	ComBanc	DCV	CCLV	ComDer	SIID-TR
Type	PS	PS	CSD	CCP/SSS	CCP	TR
Operator	BCCh	ComBanc S.A.	Deposito Central de Valores S.A.	CCLV Contraparte Central S.A.	ComDer S.A.	BCCh
Coverage	interbank	interbank	securities	various	OTC derivative	forex derivative
Established	2004	2004	1993	2010	2015	2022
Regulation	BCCh	BCCh	CMF	CMF	CMF	BCCh
Supervision	BCCh	CMF	CMF	CMF	CMF	BCCh

Source: BCCh.

Note: "Sistema LBTR" is Sistema de Liquidación Bruta en Tiempo Real and "SIID-TR" is Sistema Integrado de Información sobre Transacciones de Derivados.

15. **Chilean FMIs follow international standards for cybersecurity risk.** Chile has implemented the 'CPSS-IOSCO (Committee on Payment and Settlement Systems Technical Committee of the International Organization of Securities Commissions) Principles for Financial Market Infrastructures' (BIS, 2012) which includes information security, business continuity management, and operational risk management.[38] Additionally, the CPSS-IOSCO FSAP assessment conducted by World Bank in 2016[39] concluded that the FMIs have adopted best practices and international standards for the management of operational risks including cyber risk. All the private FMIs have certificates of ISO 22301 (Business Continuity Management) and ISO/IEC 27001 (information security management).[40] Moreover, as operator of the Sistema LBTR, the BCCh has implemented several policies and measures to enhance cyber resilience standards and also signed a Memorandum of Understanding (MoU) with other FMIs to improve coordination in this matter.

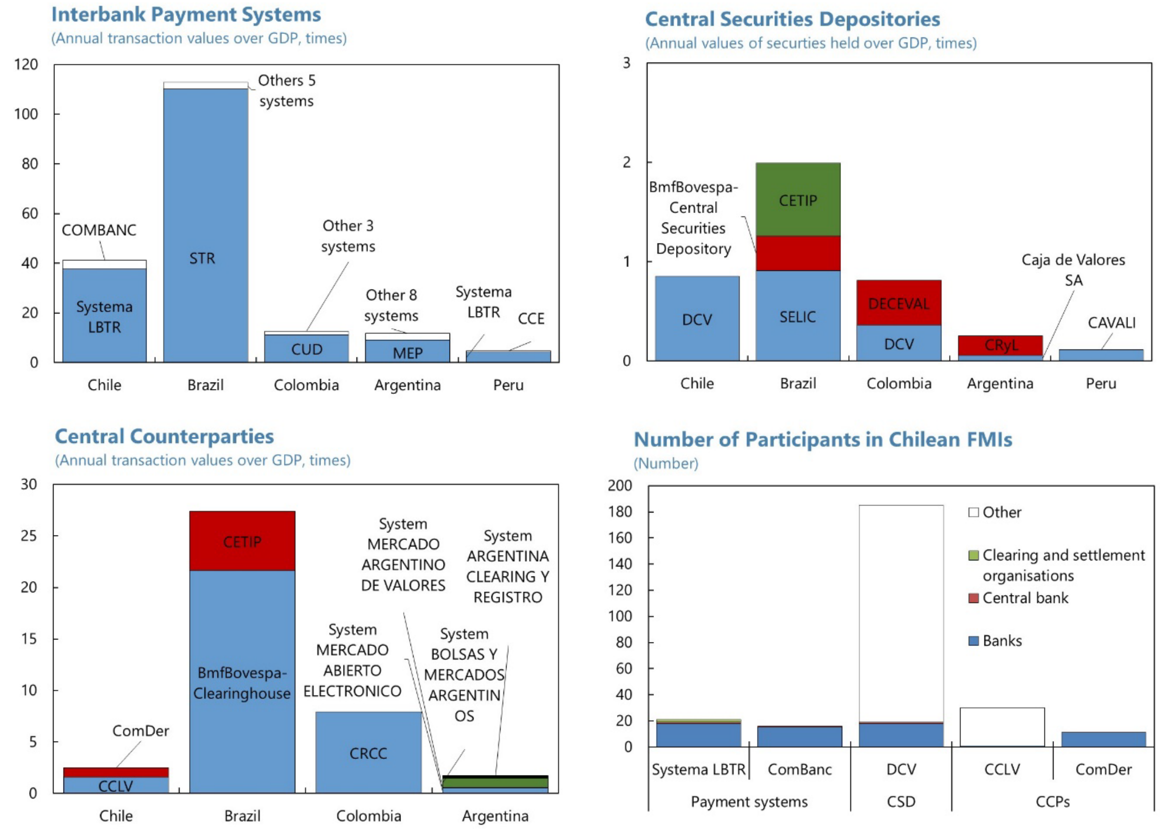
[37] These charts are created based on the 'Yellow Book Statistics,' which is the statistics about payments and financial market infrastructures in Latin American and Caribbean Countries and published by the Center for Latin American Monetary Studies (CEMLA). The methodology follows the structure of the BIS Red Book, and national central banks prepare the data with the support of CEMLA.

[38] This is based on Level 1 self-assessments. Chile has not participated in level 2 (peer review) and level 3 (peer benchmarking) assessments.

[39] The reports are available here: Systema LBTR, ComBanc, DCV, CCLV, and ComDer.

[40] In Chile, the National Institute for Standardization (INN) authenticates the ISO standards.

Figure 7. Selected Economies: Financial Market Infrastructures



Interbank Payment Systems

(Annual transaction values over GDP, times)

Central Securities Depositories

(Annual values of securties held over GDP, times)

Central Counterparties

(Annual transaction values over GDP, times)

Number of Participants in Chilean FMIs

(Number)

Sources: CEMLA and IMF staff calculations.

Note: As of 2021 except for the number of participants in CSD (as of 2019).

E. Cybersecurity Risk for the Fintech Industry

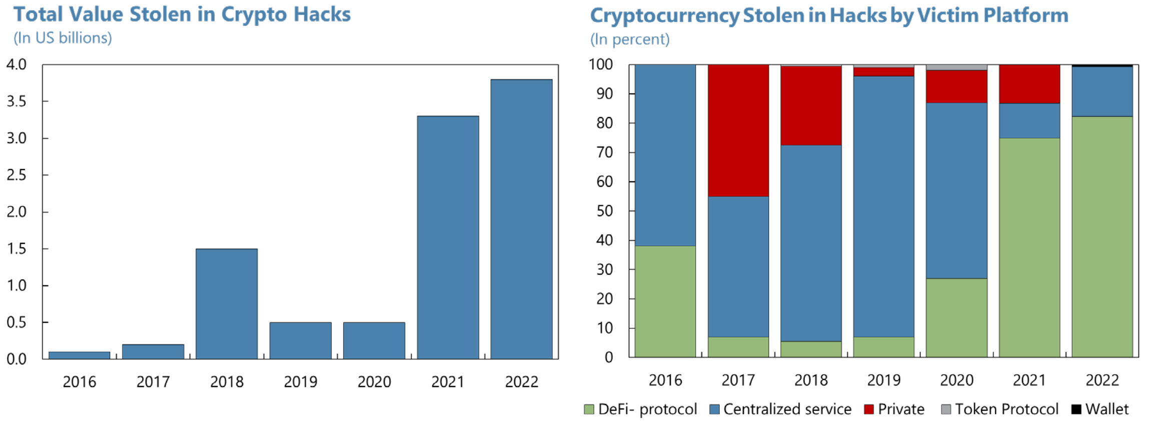
16. Fintech is considered vulnerable to cybersecurity risk due to the nature of their business. Fintech innovations are frequently exposed to cybersecurity risks due to the increased connectivity that creates numerous entry points for cyber hackers seeking vulnerabilities in the network (Lukonga 2018). This concern is particularly pertinent for client-facing applications that handle customer data (FSB, 2017b). Moreover, cyberattacks on cryptocurrencies have been rapidly increasing recently,[41] with a notable uptick in attacks on Decentralized Finance (DeFi), a crypto-market-based financial intermediation system without central intermediaries, driving this upward trend (Figure 8).[42]

[41] The charts of cryptocurrency used in this study are created based on the estimates by Chainalysis, the blockchain data platform. It should be noted that so far financial stability risk from cyberattacks on cryptocurrencies are limited. For example, global banks' exposures to cryptocurrencies are limited, according to the Basel III monitoring report in 2022.

[42] The vulnerability of DeFi to cybersecurity threats is connected to the reliance on smart contracts—computer codes stored on the blockchain and activated when specific conditions are met. All transactions occur on the blockchain,

(continued)

Figure 8. Global: Crypto Hacks

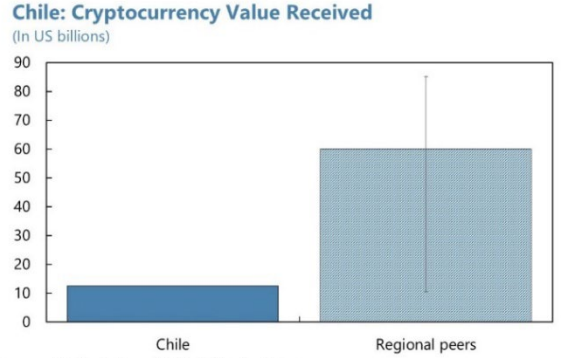


Sources: Chainalysis and IMF staff calculations.

17. The Chilean fintech firm market appears to be smaller than its regional peers but has exposures with the segment of handling a large amount of customer data.[43] Compared with regional peers, the number of fintech firms had grown more slowly, but there has been a recent substantial increase (Figure 9). The technologies used by Chilean fintech firms are concentrated on 'Open platforms &APIs' and 'Cloud computing,' which handle a big volume of customer data, and align with those utilized by its regional peers. The majority of fintech firms operating in Chile are payment and remittance systems for both domestic and foreign fintech firms,[44] and the share of payment and remittance segment in Chile is higher than its regional peers. The implementation of the Fintech Law is expected to further foster market.

18. Cybersecurity risk for Chilean financial sector through cryptocurrencies appear fairly contained. Chilean financial sector does not have meaningful exposures to cryptocurrencies. In particular, the sector has no exposure to DeFi activities. Moreover, the transaction volume of cryptocurrencies in Chile is smaller than that of regional peers. It should be noted that issuers of these currencies are global entities, which are not in the regulatory perimeter of the authorities.

Chile: Cryptocurrency Value Received



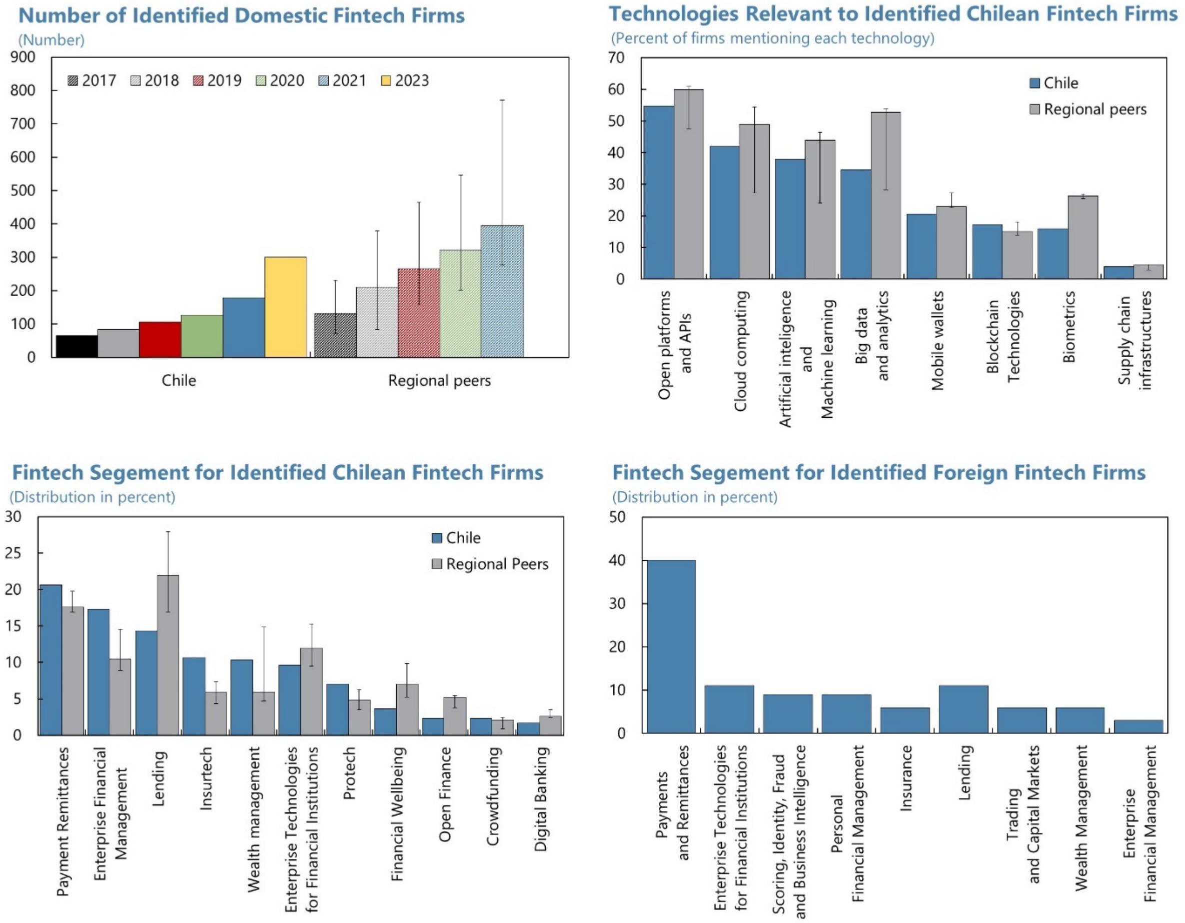
Sources: Chainalysis and IMF staff calculations.
Note: As of June 2022-July 2023. The bars and whiskers of "Regional peers" indicate the median and max/min range of Brazil, Mexico, Colombia, Argentina, and Peru.

and the codes overseeing DeFi protocols are publicly accessible. While this transparency aims to improve transactions among blockchain users, it also exposes DeFi to cybersecurity risks. Hackers can scrutinize the computer codes to pinpoint vulnerabilities and strategically exploit transaction data to maximize the impact of their cyberattacks.

[43] The charts of fintech firms used in this study are created based on the joint study by Finnovista and Inter-American Development Bank and Fintech Radars by Finnovista, which publishes research and periodical reports on the state and latest trends of Fintech innovations in Latin America.

[44] In Chile, 20 percent of operation fintech firms are foreign, most of which are Colombian, Mexican, and Argentinian.

Figure 9. Fintech Firms



Number of Identified Domestic Fintech Firms

(Number)

Technologies Relevant to Identified Chilean Fintech Firms

(Percent of firms mentioning each technology)

Fintech Segement for Identified Chilean Fintech Firms

(Distribution in percent)

Fintech Segement for Identified Foreign Fintech Firms

(Distribution in percent)

Sources: Finnovista, Inter-American Development Bank (IDB), IDB Invest, and IMF staff calculations.
Notes: As of 2023 except for "Fintech Segment for Identified Foreign Fintech Firms" (as of 2021). In the upper left panel, the bars, and whiskers of "Regional peers" indicate the median and max/min range of Brazil, Mexico, Colombia, and Argentina. In other panels, the bars, and whiskers of "Regional peers" indicate the median and max/min range of Mexico, Colombia, and Argentina. Mexico is as of 2022.

F. Regulations on Cybersecurity Risk in the Financial Sector

19. **The CMF mainly regulates the cybersecurity risk in the Chilean financial sector.** In line with global standards, Chile has adopted various initiatives to address cybersecurity risk for the nation.[45] However, the country so far has no general law or authority that address cybersecurity risk,

[45] For example, Chile published its National Cybersecurity Policy 2017-2022, with the goal of promoting a free, open, safe, and resilient cyberspace. Afterwards, in 2018, Chile established the Computer Security Incident Response Team (CSIRT) under the Ministry of the Interior and Public Security to strengthen and promote cybersecurity practices, policies, laws, regulations, protocols, and standards in state administration and critical infrastructures. Chile also joined international initiatives such as the Cyber Security Program, developed by the Organization of American States (OAS). Moreover, In June 2022, Chile introduced a computer crimes law, covering offenses like system attacks, unauthorized access, data interception, forgery, fraud, and device abuse, with penalties based on severity. In December 2023, Chile's National Cybersecurity Policy for 2023-2027 was introduced. It advocates for the establishment of the National Cybersecurity Agency and the National Registry of Cybersecurity Incidents and aims to enhance the resilience of information infrastructures and facilitate internal and international coordination.

and there is no specialized data protection authority while the relevant laws are discussed in Congress.[46] Hence, cybersecurity risk in each industry is mainly covered by sectoral regulations and the regulatory authorities.

20. The CMF has recently issued many regulations on cybersecurity risk in the financial sector, and the regulatory framework for cybersecurity risk would be comprehensive (Box 2). A stand-alone Report on the Observance of Standards and Codes for the implementation of the Basel Core Principles for Effective Banking Supervision in Chile, undertaken by the IMF and the World Bank during March-May of 2021, concluded that the Chilean regulatory framework for banks' operational risk management including cybersecurity risk is comprehensive. Moreover, the Financial Stability Council (CEF)[47] monitors and follows cyber incidents with possible systemic impact, and the CEF has an operational continuity working group (Abarca, 2023). Note that the CMF has already established a reporting and information-sharing framework and risk management requirements for banks and insurers. Additionally, plans are in place to enforce them for FMIs, fintech,[48] and fund managers. This ensures comprehensive coverage of cybersecurity risk in the financial sectors.[49]

21. Ensuring sufficient human resources for the effective cybersecurity risk supervision is critical. While the regulatory framework is comprehensive, the report above also indicated that the number of cybersecurity experts in the CMF was not sufficient to effectively conduct cybersecurity risk supervision. Ensuring sufficient budget resources for the CMF to attract and retain specialized talent was already one of the 2021 FSAP recommendations. Given that the regulatory perimeter of the CMF is expected to expand to include the fintech sector, this problem could become more serious and hinder the effectiveness of cybersecurity risk supervision. Note that the CMF's budget for cybersecurity risk supervision has incremented while total budget has decreased.

[46] The Cybersecurity and Critical Information Infrastructure Framework Bill, which aims to create a National Cybersecurity Agency and establish procedures for protecting essential services, drawing from EU regulations like NIS 1 and NIS 2 Directives, and Spain's critical information infrastructure protection rules, is discussed under the congress. The bill includes definitions for terms like cyberattack and cybersecurity and sets minimum requirements for incident prevention, containment, resolution, and response. It also proposes the creation of entities such as the National Cybersecurity Agency and the National Registry of Cybersecurity Incidents. The bill on personal data protection is discussed under Congress. The bill aligns with international standards, such as the EU's GDPR, to protect people's rights and freedoms regarding their personal data, while also proposing the establishment of a national authority for personal data protection. The National Consumer Service (SERNAC) currently manages personal data protection in consumer affairs and will do so until a dedicated data protection authority is established.

[47] The CEF was created in 2011, and it is chaired by the finance minister and includes the CMF president, the Pension Superintendent, and the BCCh Governor as a permanent invitee and advisor.

[48] Note that payment providers engaging in fintech activities are already subject to cybersecurity regulations issued by the CMF.

[49] The CMF presented detail of the regulations on FMIs in 2018 and 2023. Note that Chile received Technical Assistance on cybersecurity policies by the IMF in 2017 (Abarca, 2023).

Box 2. Recent Regulations on Cybersecurity Risk in the Financial Sector

Banks	■ In June 2016, the Superintendence of Banks, and Financial Institutions (SBIF), later known as the CMF, established the necessary requirements associated with information security and cybersecurity for the assessment of banking service providers, under the SBIF's operational risk management framework. ■ In December 2017, the SBIF introduced minimum requirements for financial institutions engaging in cloud technology outsourcing to mitigate associated risks. ■ In January 2018, the SBIF mandated cybersecurity regulations for banks. These rules require SBIF to assess critical cybersecurity infrastructure. Banks must integrate cybersecurity into operational risk management and manage critical infrastructure while maintaining a cybersecurity incident database. ■ In August 2018, the SBIF enacted cybersecurity rule changes, including a 30-minute incident reporting platform, user notification, and board involvement in cybersecurity. ■ In December 2019, the CMF modified regulations on outsourcing services for banks and financial institutions, particularly for overseas outsourcing impacting critical or strategic activities. Boards of directors became responsible for evaluating and selecting suppliers, including contingency sites, based on their needs. ■ In July 2020, the CMF implemented cybersecurity regulations effective from December 2020. These regulations apply to various financial entities and mandate Board of Directors' approval of cybersecurity strategies. Entities are required to define stages in an information security and cybersecurity risk management process, including risk identification, analysis, treatment, and incident response.
FMIs	■ In November 2022, the CMF issued regulations empowering it to supervise low-value clearinghouse administrators and set operational requirements. They include information submission requirements and provide guidelines for managing operational and cybersecurity risks, business continuity, and technology assets. ■ In August 2023, the CMF proposed regulations for consultation on corporate governance, integrated risk management, and operational risk management, which apply to FMIs and address the Board of Directors' role, policies, procedures, risk management, and operational losses and incident reporting.
Fintech	■ In February 2023, the fintech law came into effect, broadening the CMF's regulatory scope to cover various fintech activities, aiming to mitigate risks in cybersecurity and data protection. ■ In January 2024, the CMF issued regulatory requirements for financial services providers' cybersecurity management and reporting requirements, which will be effective in February 2024.
Insurers	■ In May 2021, the CMF issued operational risk management and cybersecurity standards for insurers and reinsurers, outlining instructions, and requiring periodic self-assessments as well as duties for reporting cyber incidents.
Fund managers	■ In August 2023, the CMF proposed regulations for consultation on corporate governance, integrated risk management, and operational risk management, which apply to general fund managers and address the Board of Directors' role, policies, procedures, risk management, and operational losses and incident reporting.

Sources: Financial Market Commission (CMF) and BCCh.

G. Recommendations

22. Steady implementation of the ongoing policy initiatives is warranted. The regulatory proposals for FMIs and fund managers are expected to strengthen the preparedness of the financial sector to cybersecurity risk. Implementation of the Fintech Law is also critical to address new cybersecurity risk exposures created by fintech activities while embracing the benefits from them. Moreover, the national initiatives, such as establishing the National Cybersecurity Agency and the National Registry of Cybersecurity, could also be beneficial for the financial sector, given potential spillovers from third-party service providers and importance of information sharing across industries.

23. The authorities should continue to prioritize the recruitment of additional cybersecurity experts. While the regulatory framework appears sound and comprehensive, the effectiveness of these regulations depends on the availability of supervisory resources. In this regard, the increase in the budget for cybersecurity risk supervision is welcome. As experienced with fintech, new technologies, such as AIs and quantum computing, could exacerbate cybersecurity risks for the financial sector (Shabsigh and Boukherouaa, 2023), and thus continued efforts to ensure sufficient supervisory resources are vital.

24. The authorities should consider adopting new supervisory exercises to further enhance an industry-wide crisis management framework. For instance, given the systemic nature of cybersecurity risk for Chilean financial sector, creating cyber maps of financial networks and third-party dependencies would enable the authorities to identify the critical nodes, conduct in-depth analysis of the potential impact on liquidity and solvency, and run top-down stress tests based on cyber scenarios to assess the potential impact on financial stability risks. Additionally, introducing supervisory bottom-up cybersecurity stress tests, which were initiated by the Bank of England in 2022 and are planned by the ECB for 2024,[50] could enhance the financial sector's preparedness for cybersecurity risks.

[50] Additionally, in collaboration with the IMF, the Monetary Authority of Singapore conducted bottom-up cyber stress testing on banks' capital ratios and liquidity ratios (LCRs) (Goh et al., 2020).

References

Abarca, I., 2023. "Construyendo Ciber Resiliencia en la Industria Financiera (in Spanish)." Banco Central de Chile, blog on Wednesday, May 31, 2023.

Adelmann, F., J. Elliott, I. Ergen, T. Gaidosch, N. Jenkinson, T. Khiaonarong, A. Morozova, N. Schwarz, and C. Wilson, 2020. "Cyber Risk and Financial Stability: It's a Small World After All." IMF Staff Discussion Notes 2020/007, International Monetary Fund.

Aldasoro, I., L. Gambacorta, P. Giudici, and T. Leach, 2022a. "The Drivers of Cyber Risk." Journal of Financial Stability, 60(C).

Aldasoro, I., L. Gambacorta, P. Giudici, and T. Leach, 2020b. "Operational and Cyber Risks in the Financial Sector." BIS Working Papers No 840.

Bank for International Settlement (BIS), 2012. "Principles for Financial Market Infrastructures." April 2012.

Bank for International Settlement (BIS), 2014. "Cyber Resilience in Financial Market Infrastructures." November 2014.

Bank for International Settlement (BIS), 2016. "Guidance on Cyber Resilience for Financial Market Infrastructures." June 2016.

Bank for International Settlement (BIS), 2018. "Cyber-Resilience: Range of Practices." December 2018

Bank for International Settlement (BIS), 2022a. "Business Continuity Planning at Central Banks during and after the Pandemic." April 2022.

Bank for International Settlement (BIS), 2022b. "Implementation Monitoring of the PFMI: Level 3 Assessment on Financial Market Infrastructures' Cyber Resilience." November 2022.

Bank of England (BOE), 2018. "Could a Cyber Attack Cause a Systemic Impact in the Financial Sector?" Quarterly Bulletin, 2018 Q4.

Bouveret, A, 2018. "Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment." IMF Working Paper 18/143.

Brando, D., A. Kotidis, A. Kovner, M. Lee, and S. Schreft, 2022. "Implications of Cyber Risk for Financial Stability." FEDS Notes, Board of Governors of the Federal Reserve System, May 12, 2022, Washington, DC.

Carney, M., 2019. "Enable, Empower, Ensure: A New Finance for the New Economy." Speech delivered at the Mansion House Bankers' and Merchants' Dinner, London.

Cohen, R., and J. Humphries, S. Veau, and R. Francis, 2019. "An Investigation of Cyber Loss Data and Its Links to Operational Risk." Journal of Operational Risk, 14(3).

Crosignani, M., M. Macchiavelli, and A. Silva, 2023. "Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains." Journal of Financial Economics, 147, pp. 432-448.

Duffie, D. and J. Younger, 2019. “Cyber Runs.” Hutchins Center Working Paper 51, The Brookings Institution.

Eisenbach, T., A. Kovner, and M. Lee, 2022. “Cyber Risk and the U.S. Financial System: A pre-Mortem Analysis.” Journal of Financial Economics, 145(3), pp. 802-826.

Eisenbach, T., A. Kovner, and M. Lee, 2023. “When It Rains, It Pours: Cyber Risk and Financial Conditions.” Staff Reports 1022, Federal Reserve Bank of New York.European Systemic Risk Board (ESRB), 2020. “Systemic Cyber Risk.” February 2020.

Florackis, C., C. Louca, R. Michaely, and M. Weber, 2023. “Cybersecurity Risk.” The Review of Financial Studies, 36 pp. 351-407.

The Board of Governors of the Federal Reserve System (FRB), 2021. “Cybersecurity and Financial System Resilience Report.” September 2021.

Financial Stability Board (FSB), 2017a. “Stocktake on Cybersecurity Regulatory and Supervisory Practices.” October 2017.

Financial Stability Board (FSB), 2017b. “Financial Stability Implications from FinTech.” June 2017.

Financial Stability Oversight Committee (FSOC), 2022. “Annual Report.”

Goh, J., H. Kang, Z. Koh, J. Lim, C. Ng, G. Sher, and C. Yao, 2020. "Cyber Risk Surveillance: A Case Study of Singapore." IMF Working Papers 2020/028, International Monetary Fund.

Harry, C., and N. Gallagher, 2018. “Classifying Cyber Events.” Journal of Information Warfare, 17(3), pp. 17-31.

Healey, J., P. Mosser, K. Rosen, and A. Tache, 2018. “The Future of Financial Stability and Cyber Risk.” mimeo.

He, Z., S. Jiang, D. Xu, and X. Yin, 2023. “Investing in Lending Technology: IT Spending in Banking.” NBER Working Paper No. 30403.

Jamilov, R., H. Rey, and A. Tahoun, 2021. “The Anatomy of Cyber Risk.” mimeo.

Lukonga, I., 2018. "Fintech, Inclusive Growth and Cyber Risks: Focus on the MENAP and CCA Regions." IMF Working Papers 2018/201, International Monetary Fund.

Modi, K., N. Pierri, Y. Timmer, M. Soledad Martinez Peria, 2022. “The Anatomy of Banks’ IT Investments: Drivers and Implications.” IMF Working Paper 22/244.

Montoya, A., and R. Celedon, 2021. “Guidelines for the Development of an Open Finance Framework in Chile, with a Focus on Competition and Financial Inclusion.” August 2021, Ministerio de Hacienda.

Shabsigh, G., and E. Boukheroua, 2023, “Generative Artificial Intelligence in Finance: Risk Considerations.” International Monetary Fund, Fintech Notes, 2023/006.

FINTECH AND FINANCIAL INCLUSION IN CHILE[1]

Chile is a regional leader in financial inclusion, but it still lags behind its OECD peers. Developments in the fintech sector have the potential to further enhance financial inclusion in Chile by providing financial services to unbanked entities, lowering financial service costs, and creating more suitable financial services. The Fintech Law aims at fostering the fintech sector by bringing transparency and resiliency to the sector with new regulations, and by establishing an open finance system that reduces information asymmetry.

A. Challenges in Financial Inclusion

1. **Chile has already achieved relatively high access to financial products and services, but coverage is not yet complete.** About 85 percent of Chileans had access to accounts at financial institutions and used digital payments compared to around 50 percent in 2011 and 2014 (Figure 1). Also, disparities in access based on gender, age, and income levels are minimal. However, individuals with lower education levels, those residing in rural areas, and those not currently in the labor force are less likely to have access to these products and services.

2. **The actual use of savings and loans lags behind OECD peers.** A notable gap persists in comparison with OECD averages. As discussed in 2021 FSAP, the discrepancy between consumer preferences and the available financial products and services in the market, coupled with a lack of financial literacy among consumers,[2] may contribute to this gap.

3. **The authorities have deployed several initiatives to enhance financial inclusion.** Historically, the state-owned bank Banco Estado has played a crucial role in improving financial inclusion in Chile by providing accounts to large segments of the population (Gershenson et al., 2021). In 2006, the bank introduced Cuenta RUT, which is a demand account featuring simplified opening procedures, no income prerequisites, and no maintenance fees. Today Banco Estado provides about 14.5 million Cuenta RUT accounts (equivalent to about 95 percent of the adult population). Other initiatives for more financial inclusion are, for example, the publication of the National Financial Education Strategy by the Advisory Commission for Financial Inclusion,[3] and the ongoing development of a national financial inclusion strategy. Furthermore, on the financial policy

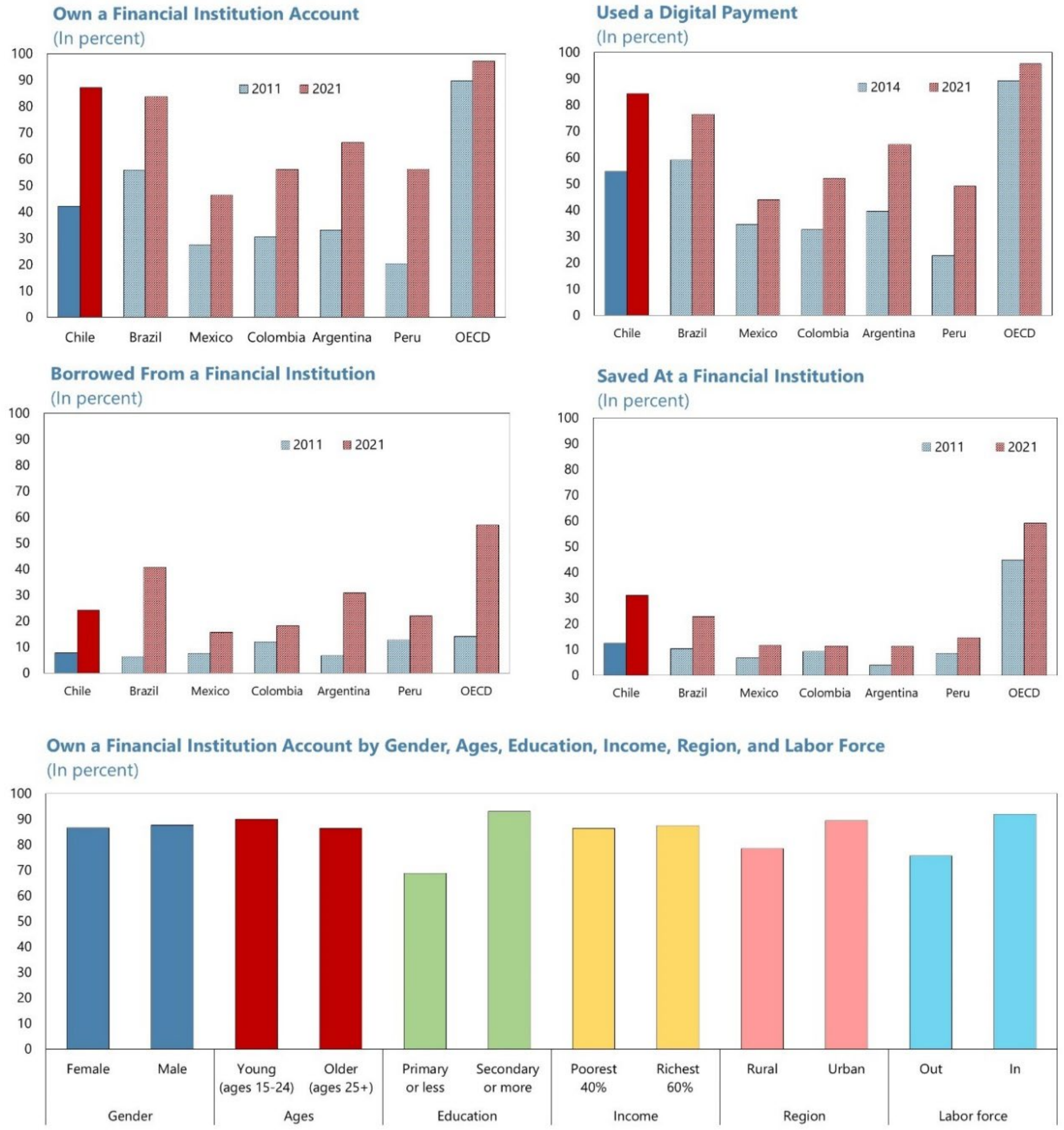
[1] Prepared by Tatsushi Okuda. The author would like to thank the BCCh and CMF staff for helpful information.

[2] Financial literacy scores in Chilean students tend to be lower than OECD averages (OECD, 2018; OECD 2015).

[3] The National Financial Inclusion Council, established in 2014, coordinates policymaking and advises the President on the National Strategy for Financial Inclusion and Consumer Protection.

front, the authorities introduced regulations, including to simplify the transfer between service providers and regulate payment card interchange fees.[4]

Figure 1. Financial Inclusion



Own a Financial Institution Account
(In percent)

Used a Digital Payment
(In percent)

Borrowed From a Financial Institution
(In percent)

Saved At a Financial Institution
(In percent)

Own a Financial Institution Account by Gender, Ages, Education, Income, Region, and Labor Force
(In percent)

Sources: World Bank and IMF staff calculations.
Note: "OECD" represents the averages in the groups. The responses are individuals aged over 15. The numbers for Mexico in 2021 are those in 2022. "Used a Digital Payment", "Borrowed From a Financial Institution", and "Saved At a Financial Institution" are usages of the products and services in the last year.

[4] Among others, in 2020, the Financial Portability Law was implemented, simplifying the process for individuals and businesses to transfer between service providers for financial services, including bank accounts, credit cards, mortgages, and loans. Additionally, in 2021, the Market Agents Law was enacted, establishing new transparency requirements, and reinforcing the responsibilities of market agents, with the aim of promoting competition and enhancing financial consumer protection. In parallel, the Interchange Fee Law was implemented to regulate payment card interchange fees.

B. Role of Fintech in Financial Inclusion

4. The authorities have deployed several initiatives to enhance Fintech could improve financial inclusion in various ways. In general, the development of the fintech sector is regarded to enhance consumers' financial access by providing tailored financial product and services (Feyen et al., 2021), decreasing asymmetric information using a larger amount of data (Philippon, 2019 and Yang and Zhang, 2022), and lowering cost of financial services by strengthening competition (Bakker et al., 2023).

5. The Chilean fintech sector is rapidly growing. According to Fintech Radar Chile, as of 2023, there are 300 Chilean fintech companies, marking a significant increase from 179 in 2021 (Figure 2). Regarding segment distribution, payment, and remittances fintech is the largest, followed by enterprise financial management. There also exist 78 foreign (e.g., Colombian, Mexican, and Argentinian) fintech firms operating in Chile. Around one third of fintech firms in Chile target consumers as customers, while the rest targets businesses. In terms of size, the distribution is grouped into two main bands: (i) the range from 1 to 100 thousand USD, and (ii) the range from 1 to 4 million USD. The technologies utilized by these firms are mainly open platforms and APIs, followed by cloud computing and artificial intelligence and machine learning. About 70 percent of Chilean fintech firms have raised capital from third parties, including angel investors, family, and friends.

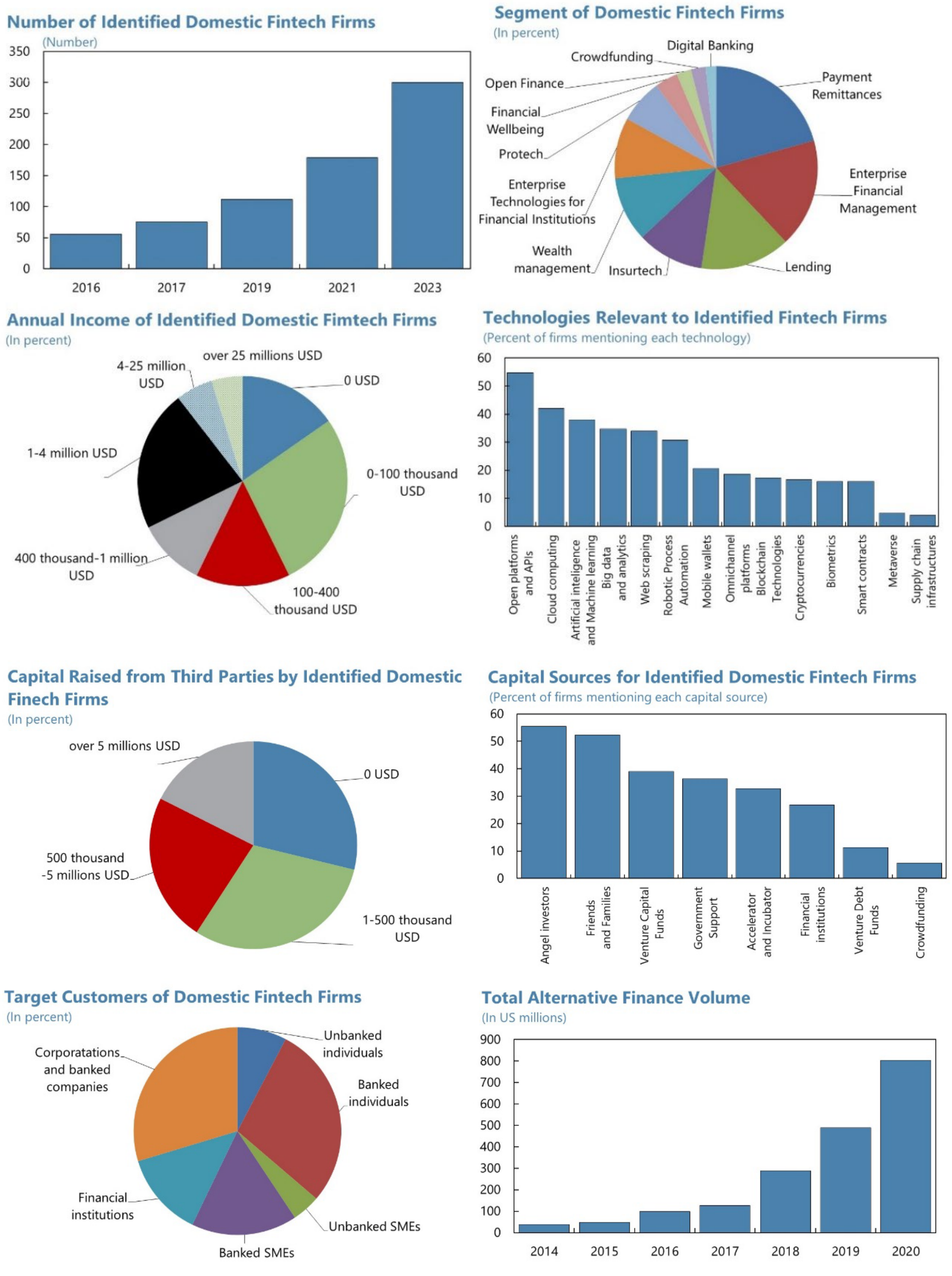
6. Fintech firms are reaching out to unbanked people, and they could contribute to financial inclusion by supplying lower-cost and more tailored financial products and services. In Chile, because Banco Estado provide bank accounts and digital banking to majority of the people, products and services targeting unbanked individuals and SMEs are rare (8 and 4 percent, respectively). Nonetheless, according to Montoya and Celedon (2021), more than half of Fintech companies reported having unbanked or underbanked[5] individuals or companies among their clients and believe that they contribute to financial inclusion by providing lower-cost financial products and services that better suit their customers' needs. Moreover, according to the report by Cambridge Center for Alternative Finance, Chilean alternative finance market, primarily composed of invoice trading[6] and facilitated by fintech firms through online platforms, has been growing.[7]

[5] "Underbanked" refers to individuals who have access to some basic financial services or a bank account but lack access to a complete suite of financial offerings.

[6] Invoice trading allows companies to borrow money from investors using unpaid or overdue invoices as collateral. Facilitated by Invoice Trading platforms, companies can sell these invoices to online investors for financing.

[7] This segment is still marginal at less than US$1 billion in 2020 compared to bank loans of around US$ 250 billion in the same year.

Figure 2. Fintech Industry



Number of Identified Domestic Fintech Firms
(Number)

Segment of Domestic Fintech Firms
(In percent)

Annual Income of Identified Domestic Fimtech Firms
(In percent)

Technologies Relevant to Identified Fintech Firms
(Percent of firms mentioning each technology)

Capital Raised from Third Parties by Identified Domestic Finech Firms
(In percent)

Capital Sources for Identified Domestic Fintech Firms
(Percent of firms mentioning each capital source)

Target Customers of Domestic Fintech Firms
(In percent)

Total Alternative Finance Volume
(In US millions)

Sources: Cambridge Center for Alternative Finance, Finnovista, and IMF staff calculations.
Note: As of 2023.

C. Fintech Law

7. **The Fintech Law aims at fostering the fintech sector and could further enhance financial inclusion.** The law, which became effective in February 2023, also aims to promote competition and financial innovation, improve customer protection, data protection, and cybersecurity, and prevent money laundering and financing of terrorism. It consists of three key elements: (i) regulating fintech activities, (ii) establishing an open finance system, and (iii) regulating crypto assets.

8. **Firms engaging in fintech activities are regulated by the CMF.** Specifically, under the new Fintech Law, the CMF issues regulations, including licensing, required risk management, disclosure requirements, and data protection measures of the following five types of fintech activities: (i) platforms for collective financing of loans or investment (crowdfunding), (ii) alternative trading systems, (iii) custody service of financial instruments, (iv) credit and investment advisory services, and (v) trading of financial instruments, and transaction routing.[8] These regulations aim to foster the fintech sector by enhancing transparency and resiliency within the sector. They also have the potential to attract more investment into fintech firms, which heavily rely on funding from third parties. The CMF will also issue regulations to establish information requirements for the supervision of fintech activities.

9. **The operation and implementation of the open finance system will be mainly regulated by the CMF.**[9] The law enables customers to share their financial information (with banks, payment card issuers, etc.) with new service providers, including fintech firms (information-based service providers and payment initiators), while retaining greater control over their financial data. The CMF will issue regulations covering areas such as risk management, cybersecurity, technical standards, cost distributions, payment initiations, and consents. Additionally, the CMF will actively participate in determining technical specifications and manuals. Payment initiators that temporarily hold clients' money in their operations will also be subject to regulation by the BCCh. The open finance system has the potential to address information asymmetry and streamline the development of new financial products and services.

10. **Financial services related to crypto assets will be regulated by the CMF while stablecoins will be subject to the BCCh regulations.**[10] The law stipulates that crypto assets, exchanges, and related intermediaries will be subject to regulation by the CMF. In contrast, stablecoins (crypto assets whose value is pegged to specific currencies, such as the U.S. dollar) are treated as a payment method and fall under the BCCh regulation, as long as they are issued in Chile by entities supervised by the CMF.

[8] They order buying or selling financial instruments for third parties, or channeling said orders to alternative transaction systems or stock or product brokers.

[9] For details, see Montoya and Celedon (2021).

[10] Regarding the presence of crypto assets in Chile, Chainalysis reports that the usage and adoption level of crypto assets are estimated to be limited and lower than those of regional peers.

11. The authorities have started the implementation of Fintech Law, which came into force in February 2023.[11] Regarding regulation of new financial activities, based on feedbacks from interested parties during the consultation phase, in January 2024, the CMF issued the regulations for fintech companies and related services, which imposes a variety of requirements on fintech firms such as registration, authorization, information disclosures, risk management, and prudential measures. The regulations will be effective in February 2024. In terms of the open finance system, in October 2023, the CMF started consultation roundtables, aimed at establishing the operational and legal design of the system and technical standards as well as regulatory guidelines including risk management. In July 2023, pursuant to its Payments regulatory Agenda, the BCCh published its proposal to update prudential regulations on payment cards, to incorporate new business models that participate in the system. Going forward, relevant regulations to fully implement the law must be issued by the CMF within 18 months or by July 2024, and the CMF estimates that approximately 70 regulations will be issued through this process. After that, participants of the open finance system are expected to implement the system by the first half of 2027.[12] In turn, in 2024, the BCCh plans to issue regulation on payment initiation services, in line with rules to be defined by the CMF for the open finance system.

12. A thorough communication is crucial for smoothly implementing the law. Throughout the implementation process, the authorities are striving to ensure it is public, transparent, and participative, utilizing various avenues such as consultation roundtables. This is crucial due to the potential for conflicts of interest among entities in the financial sector arising from the implementation of this law. For example, while the financial stability risk posed by various entities, such as banks and fintech firms, may so far differ, regulations should ensure a level of symmetry to foster fair competition in the market and bolster the resilience of the financial system amid future developments in the fintech sector. Furthermore, establishing and maintaining an open financial system could entail additional costs, making fair cost-sharing among participants essential.

[11] Regulation on crypto assets, exchanges and related intermediaries are included in those for fintech activities. In terms of the stablecoins, they are subject to the BCCh regulation only if the respective issuers are established in Chile, and thus developing a new regulatory framework for them is not a BCCh's priority in the short-term while the bank will continue to review international experiences and hold meetings with private sector actors.

[12] Open Finance System Forum includes members from the financial sector and is consultation body to the CMF. It will provide proposals on technical specifications and manuals.

References

Bakker, B., B. Garcia-Nunes, W. Lian, Y. Liu, C. Perez Marulanda, A. Siddiq, M. A. Sumlinski, Y. Yang, and D. Vasilyev, 2023. "The Rise and Impact of Fintech in Latin America." International Monetary Fund, Fintech Notes No 2023/003.

Feyen, E., J. Frost, L. Gambacorta, H. Natarajan, and M. Saal, 2021. "Fintech and the Digital Transformation of Financial Services: Implications for Market Structure and Public Policy." BIS Papers, No 117.

Gershenson, D., F. Lambert, L. Herrera, G. Ramos, M. Rousset, and J. Torres, 2021. "Fintech and Financial Inclusion in Latin America and the Caribbean" IMF Working Paper No. 2021/221.

Montoya, A. M., and R. Celedon, 2021. "Guidelines for the Development of an Open Finance Framework in Chile, with a Focus on Competition and Financial Inclusion." Chilean Ministry of Finance, 2021 August.

Philippon, T., 2019. "On Fintech and Financial Inclusion." National Bureau of Economic Research Working Paper Series, No. 26330.

Yang, T., and X. Zhang, 2022. "FinTech Adoption and Financial Inclusion: Evidence from Household Consumption in China." Journal of Banking and Finance, Volume 145,106668.