PROJECT SYNDICATE

What's wrong with negative rates?

BUSINESS & FINANCE

JOSEPH E. STIGLITZ

I wrote at the beginning of January that economic conditions this year were set to be as weak as in 2015, which was the worst year since the global financial crisis erupted in 2008. And, as has happened repeatedly over the last decade, a few months into the year, others' more optimistic forecasts are being revised downward.

The underlying problem – which has plagued the global economy since the crisis, but has worsened slightly – is lack of global aggregate demand. Now, in response, the European Central Bank (ECB) has stepped up its stimulus, joining the Bank of Japan and a couple of other central banks in showing that the "zero lower bound" – the inability of interest rates to become negative – is a boundary only in the imagination of conventional economists.

And yet, in none of the economies attempting the unorthodox experiment of negative interest rates has there been a return to growth and full employment. In some cases, the outcome has been unexpected: Some lending rates have actually increased.

It should have been apparent that most central banks' pre-crisis models – both the formal models and the mental models that guide policymakers' thinking – were badly wrong. None predicted the crisis; and in very few of these economies has a semblance of full employment been restored. The ECB famously raised interest rates twice in 2011, just as the euro crisis was worsening and unemployment was increasing to double-digit levels, bringing deflation ever closer.

They continued to use the old discredited models, perhaps slightly modified. In these models, the interest rate is the key policy tool, to be dialed up and down to ensure good economic performance. If a positive interest rate doesn't suffice, then a negative interest rate should do the trick.

It hasn't. In many economies – including Europe and the United States – real (inflation-adjusted) interest rates have been negative, sometimes as much as -2 percent. And yet, as real interest rates have fallen, business investment has stagnated. According to the OECD, the percentage of GDP invested in a category that is mostly plant and equipment has fallen in both Europe and the US in recent years. (In the US, it fell from 8.4 percent in 2000 to 6.8 percent in 2014; in the EU, it fell from 7.5 percent to 5.7 percent over the same period.) Other data provide a similar picture.

Clearly, the idea that large corporations precisely calculate the interest rate at which they are willing to undertake investment – and that they would be willing to undertake a large number of projects if only interest rates were lowered by another 25 basis points – is absurd. More realistically, large corporations are sitting on hundreds of billions of dollars – indeed, trillions if aggregated across the advanced economies – because they already have too much capacity. Why build more simply because the interest rate has moved down a little? The small and medium-size enterprises (SMEs) that are willing to borrow couldn't get access to credit before the ECB went negative, and they can't now.

Simply put, most firms – and especially SMEs – can't borrow easily at the T-bill rate. They don't borrow on capital markets. They borrow from banks. And there is a large difference (spread) between the interest rates the banks set and the T-bill rate. Moreover, banks ration. They may refuse to lend to some firms. In other cases, they demand collateral (often real estate).

> *The big lesson from all of this is captured by the familiar adage, "garbage in, garbage out." If central banks continue to use the wrong models, they will continue to do the wrong thing.*

It may come as a shock to non-economists, but banks play no role in the standard economic model that monetary policymakers have used for the last couple of decades. Of course, if there were no banks, there would be no central banks, either; but cognitive dissonance has seldom shaken central bankers' confidence in their models.

The fact is that the eurozone's structure and the ECB's policies have ensured that banks in the underperforming countries, and especially in the crisis countries, are very weak. Deposits have left, and the austerity policies demanded by Germany are prolonging the aggregate-demand shortfall and sustaining high unemployment. In these circumstances, lending is risky, and banks have neither the appetite nor ability to lend, particularly to SMEs (which typically generate the highest number of jobs).

A decrease in the real interest rate – that on government bonds – to -3 percent or even -4 percent will make little or no difference. Negative interest rates hurt banks' balance sheets, with the "wealth effect" on banks overwhelming the small increase in incentives to lend. Unless policymakers are careful, lending rates could increase and credit availability decline.

There are three further problems. First, low interest rates encourage firms to invest in more capital-intensive technologies, resulting in demand for labour falling in the longer term, even as unemployment declines in the short term. Second, older people who depend on interest income, hurt further, cut their consumption more deeply than those who benefit – rich owners of equity – increase theirs, undermining aggregate demand today. Third, the perhaps irrational but widely documented search for yield implies that many investors will shift their portfolios toward riskier assets, exposing the economy to greater financial instability.

What central banks should be doing is focusing on the flow of credit, which means restoring and maintaining local banks' ability and willingness to lend to SMEs. Instead, throughout the world, central banks have focused on the systemically significant banks, the financial institutions whose excessive risk taking and abusive practices caused the 2008 crisis. But a large number of small banks in the aggregate are systemically significant – especially if one is concerned about restoring investment, employment, and growth.

The big lesson from all of this is captured by the familiar adage, "garbage in, garbage out." If central banks continue to use the wrong models, they will continue to do the wrong thing.

Of course, even in the best of circumstances, monetary policy's ability to restore a slumping economy to full employment may be limited. But relying on the wrong model prevents central bankers from contributing what they can – and may even make a bad situation worse.

The writer is a Nobel laureate in economics, and Professor at Columbia University. His most recent book, co-authored with Bruce Greenwald, is *Creating a Learning Society: A New Approach to Growth, Development, and Social Progress*.

INDUSTRIAL HACKING

A real and significant danger

DITTO SYED HAQ

PHOTO: **SECURITYINTELLIGENCE**

With news of the $101 m heist at Bangladesh Bank making headlines around the world, both the global Financial Services sector and regulators will be watching events closely as they unfold. That the perpetrators were able to successfully bypass a complex multi-stage biometric verification process is itself cause for concern and could call into question the effectiveness of such authentication methods as criminals are adopting increasingly sophisticated means to circumvent them. Once the mainstay of solitary individuals and disaffected youth, "industrial hacking" is now a real and significant danger with backing from international organised crime and the stakes, as we have seen, are frighteningly high.

In the absence of solid evidence, one can still form a broad picture of the means by which the incident at Bangladesh Bank had occurred. Firstly, the encrypted and highly secure mechanism of SWIFT transfers between their dedicated terminals means that the likelihood of communications being intercepted or tampered en route can be ruled out. Secondly, that the recipient institution cannot initiate transactions from their end would exclude the possibility of any technical breach on that side. Given that the systems within Bangladesh Bank are themselves protected against external intrusion attempts by enterprise-grade firewall software, this leaves us with the unsettling conclusion that the crime is mostly likely to have occurred from within, prompting a line of investigation that is actively being pursued as we speak. While it would be unwise to draw further conclusions while the investigation is underway, the incident drives home the realities and challenges faced by the financial services industry as a whole.

Consulting firm Accenture, in their Global Risk Management Study of Investment Banking in 2015, revealed that 65 percent of Financial Services executives believed that cybercrime and IT risk would have an increased impact on their business in the next two years. Worryingly, it was also revealed that less than 10 percent of those institutions proactively ran inward-directed simulations of cyber-attacks or intentional failures to test the resilience of their systems against such events. Such a low level of cyber-threat awareness and preparedness combined with the astronomical sums of money involved makes members of the financial services industry prime targets for organised electronic crime on an unprecedented scale. It also demonstrates that cybercrime is a threat perceived by the entire global banking community and not Bangladesh alone.

A separate study by Accenture in conjunction with Ponemon Group, also in 2015, revealed that organisations at the forefront in the fight against cybercrime shared certain common traits. One of these was the appointment of a Chief Information Security Officer or CISO who would report directly to the CEO and board of directors to ensure that breaches of systems security were addressed at the top levels of organisations as a matter of top priority. It also noted that such firms were actively engaged in the on-going development of an overall IT security strategy along with clear definitions of security roles and responsibilities which were then communicated to employees at all levels. Four "Big Picture Principles" were identified: having a proactive stance, taking a broad view of risk management, a willingness to collaborate and, paying attention to the "human factor".

It is this last point, the "human factor" that is the most difficult for organisations to identify and control. The touch-points between humans and computers will always continue to be the weakest link in ensuring the integrity and security of any computer system and, unsurprisingly, an overwhelming majority of hacking incidents are attributed to human intervention in some form. This could be down to something as simple as accepting a prompt to install malicious software, browsing a compromised website or inserting an infected USB flash drive into a target machine. Such incidents often indicate a breakdown in internal control structures such as the appropriate segregation of duties or vetting of staff with access to critical systems. In the case of Bangladesh Bank, this is likely to be one of the key areas of focus for investigators and something that will be followed by stakeholders and the industry at large.

While it is easy to point out lapses that may or may not have occurred at Bangladesh Bank, it is important to note that the burden of responsibility for cybercrime is a shared one. Each and every party involved in the generation, handling and processing of financial data has a collective duty of care to ensure that only legitimate and verifiable transactions pass through the financial system. That is the main purpose of the comprehensive anti money-laundering awareness programmes that institutions require their staff to undertake on a regular basis. Importantly, this type of training is not restricted to front-office operatives alone, but applicable to all staff who are in contract with the physical or electronic trail of money throughout the lifetime of the transaction cycle. This implies that rather than a single point of failure, there may have been multiple issues relating to people and process in the organisations concerned that resulted in a significant number of fraudulent transactions passing through the system unchallenged.

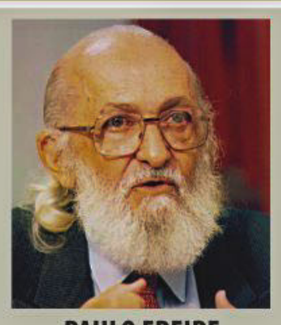
It is because of this shared burden of care and responsibility that all institutions involved should make a joint effort to get to the bottom of the matter. While there may not have been a technical breach of systems within the Federal Reserve, there were perhaps issues around due diligence that need to be looked into to prevent further incidents such as this. That multiple sequential payments to different accounts from the reserve account of a sovereign nation would be made without being investigated is extremely worrying. Also, the fact that the $101m in question reputedly represents a subset of a much larger amount requested to be withdrawn at the same time - requests that were subsequently declined - demands that the Fed look into their evaluation criteria for the assessment and identification of fraudulent activity on their client accounts.

Being able to identify and isolate suspicious transactions, no matter how legitimate they may seem, is at the heart of the trust that both people and governments worldwide place in financial institutions whom they entrust to be custodians of their hard-earned money. Whether the end customer is an individual or a nation, banks have a duty to safeguard customer and transactional information as well as monitor activity on their customer accounts to identify and prevent unauthorised or criminal activity. For example, the next time you are abroad and your credit card gets declined for seemingly no reason, it is probably because banks are doing their job properly.

But customers are not the only ones to benefit from such preventive measures. The significant cost to financial institutions of implementing robust and effective systems security is overshadowed by the damage to reputation and monetary loss they could face in the event of a breakdown. The widely publicised ATM hacking operation involving three of Bangladesh's prominent retail banks that was foiled just weeks before the Bangladesh Bank incident is a point in case. Whatever the outcome of current investigations, these incidents call for a heightened awareness of the need to review and improve existing controls in order to retain the confidence of a disillusioned public in the financial system. In doing so, it should be remembered that effective cyber security begins at the top and it is only by driving down radical change in mind-set from the highest levels of the organisation that we can prevent a repeat occurrence of such events.

The writer is CEO and Principal Consultant at Indigo ICT, a Dhaka-based firm specialising in business technology.

QUOTABLE *Quote*



PAULO FREIRE

It is not the unloved who initiate disaffection, but those who cannot love because they love only themselves. It is not the helpless, subject to terror, who initiate terror, but the violent, who with their power create the concrete situation which begets the 'rejects of life.' It is not the tyrannized who initiate despotism, but the tyrants. It is not those whose humanity is denied them who negate humankind, but those who denied that humanity (thus negating their own as well).

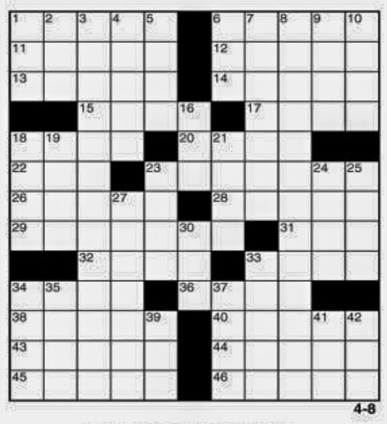
CROSSWORD BY THOMAS JOSEPH

ACROSS

1 Despise
6 Indy events
11 Game token
12 Eat away
13 Studied
14 Tigger's creator
15 Sunup site
17 Cain's father
18 Related
20 "Back in Black" band
22 Fizz ingredient
23 Resolve
26 Chaser of Bugs
28 Viola's cousin
29 Drink for the lactose intolerant
31 Genetic stuff
32 Garden aid
33 Herring's kin
34 Yard divisions
36 Blockhead
38 Benefit
40 Organ's cousin
43 Enthusiasm
44 Cupid's missile
45 Pays to play
46 Door holder's words

DOWN

1 Phone download
2 Book jacket bit
3 # 1 hit for Al Martino
4 Shark's home
5 Cincinnati team
6 "Stand" band
7 She helped Theseus
8 #1 hit for Tony Bennett
9 Writer Ferber
10 Appear
16 Seaman
18 Historic times
19 Metric mass
21 Fighting bird
23 Fancy flower
24 Arm bone
25 Swamp croaker
27 Hammy, say
30 Went ahead
33 Church feature
34 Bean variety
35 Tied up
37 Lustrous stone
39 French article
41 -- de plume
42 Need to pay



4-8

YESTERDAY'S ANSWER

A	B	U	T		B	O	B	S	U	P
W	A	N	E		U	N	E	A	S	E
L	I	F	T		M	E	A	G	E	R
S	T	O	O	D	P	A	T			
		U	N	O		C	L	U	B	S
R	I	N	S	E		T	E	N	E	T
O	D	D						B	A	A
A	L	E	R	T		A	D	O	R	N
M	E	D	E	A		L	O	U		
		P	T	B	A	R	N	U	M	
D	E	S	O	T	O		E	D	N	A
E	R	A	S	E	D		M	E	D	S
W	A	T	E	R	Y		I	D	O	S

BEETLE BAILEY by Mort Walker

BABY BLUES by Kirkman & Scott