WSJ AIMS TO RESTORE CONFIDENCE IN SWIFT … BY REMAINING SILENT ABOUT RISKS FROM NSA

WSJ has a 2000 word puff piece talking about how the international financial messaging system, SWIFT, is safe from hackers now because more banks are using two-factor authentication (!!) with the system that can transfer billions of dollars with each message.

> The bank also wasn't using two-factor authentication on the system it used to access Swift, according to a person familiar with the bank's procedures. Two-factor authentication is a higher security standard that requires a second measure of verification in addition to a password.
>
> Software that Swift provides to customers now has built-in two-factor authentication, but they can opt not to use it. At the time of the Bangladesh cyberattack, two-factor authentication was merely Swift's preference for local access, according to a copy of its security guidance reviewed by The Wall Street Journal.
>
> Two people briefed on the theft say two-factor authentication might not have made the hacks impossible but would have made them more difficult.
>
> [snip]
>
> Within days [of the Bangladesh hack], Swift rolled out a new customer security program, hinting that it wouldn't rule out the possibility of kicking violators out of the network. Swift didn't make the controls mandatory until September.
>
> The 16 mandatory standards include

> tighter password security, such as two-factor authentication. Swift ordered bank customers to update software, threatening to report to regulators anyone who doesn't obey. Regulators have the power to withdraw licenses from banks deemed insufficiently safe and sound.
>
> Axletree's Mr. Murali says the number of clients he works with who have requested two-factor authentication for the Swift messaging system has jumped to about 150 from 10 since last year.
>
> Swift will likely need more time to fully win back confidence. The New York Fed stopped making payments on the strength of Swift messages alone and adopted a policy of double-confirming orders from Bangladesh by phone.

But the piece on the recent hacks — it discusses Bangladesh and Ecuador specifically, but mentions 26 total attempted attacks, though claims the other 24 were unsuccessful — remains utterly silent about the background to the hacks by thieves: the hack by NSA, which was first exposed in 2013, but recently exposed in far more detail in a Shadow Brokers dump.

I mean, sure, financial systems that can affect billions of dollars should have 2FA!

But it's likely the thieves figured out SWIFT's vulnerabilities thanks to the exposed NSA hacks.