DEFUND FINANCIAL CYBER SECURITY

BY GIDEON SAMID
gideon@bitmint.com

CYBER FRAUD IS ENDEMIC. No one is immune. The Federal Office of Budget and Management, the National Security Agency, political campaigns, all have been victimized. It's the same for financial institutions—but with one subtle distinction that makes all the difference in the world.

Let me explain. No harm is inflicted on me on account of my Social Security number having been exposed. Unlike a hidden bad habit or an embarrassing criminal record, a piece of financial data does not reflect ill on me. I am okay with you knowing my account number, even my password, as long as you cannot use this knowledge to harm me.

So, instead of piling up technology to protect my financial data from exposure, why not invoke technology to make it impossible for a fraudster to use this exposure to steal my identity? Once such a solution is deployed, the multi-billion dollar cyber security industry, or the part thereof that preys on fear, will dissolve and disappear.

To explain the concept, let's invoke a well-known tale from the world of espionage. Storied spies were instructed to introduce one or two spelling errors into their radioed reports. When they were caught and forced to send false messages, they sent error-free scripts, thereby signaling to the home base that they had been compromised.

Now suppose information submitted by a customer to a merchant is ever so slightly different from the respective data held by the merchant. In the event the merchant is hacked, and the hacked credentials are submitted to steal an identity, then the submission will look exactly as the data kept by the merchant. Instantly, the merchant will recognize it has been hacked and prevent the attempted identity theft.

Financial hackers are not ideologues. They are businessmen. One of the hackers in the 2009 Heartland break-in intimated to me the sizable investment the hackers had made, based on their expectation for a return on that investment. Once hackers realize that penetrating thick security walls yields useless gain, they will never again waste their effort on anyone similarly protected. That makes it unnecessary for the protected merchant to surround its data with super costly security.

Several technologies like this are being developed. One of them is called Nooance (see details at bitmintalk.com/nooance). Let two people jot down the same phone number. One can dial the right number reading from either note, but the handwriting will not be identical. A similar distinction has been developed for bit-wise computer language. When a hacker steals financial data from the merchant's database, he gets the right data, but not an exact copy of the same data as entered into the customer's phone. If the stolen data is submitted to claim a false identity, the merchant will spot the fraud.

The hacker will soon realize that the data he stole has no value in the marketplace. Moreover, he implicates himself and is likely to get caught. With so many vulnerable merchants relying on security walls for protection, it would be stupid for a hacker to waste his effort on an "unproductive merchant."

The Nooance technology is a simple add-on, requiring no internal changes to financial software, no refreshing of credentials, no new parameters, no interference with the prevailing financial protocols. If it's widely deployed, hackers will no longer be able to violate millions of victims via one merchant. They will have to hack the same data phone by phone.

Once a merchant becomes unattractive to cyber fraudsters, it is due time to consider defunding some unnecessary (and burdensome) cybersecurity walls, simplifying the payment process. DT