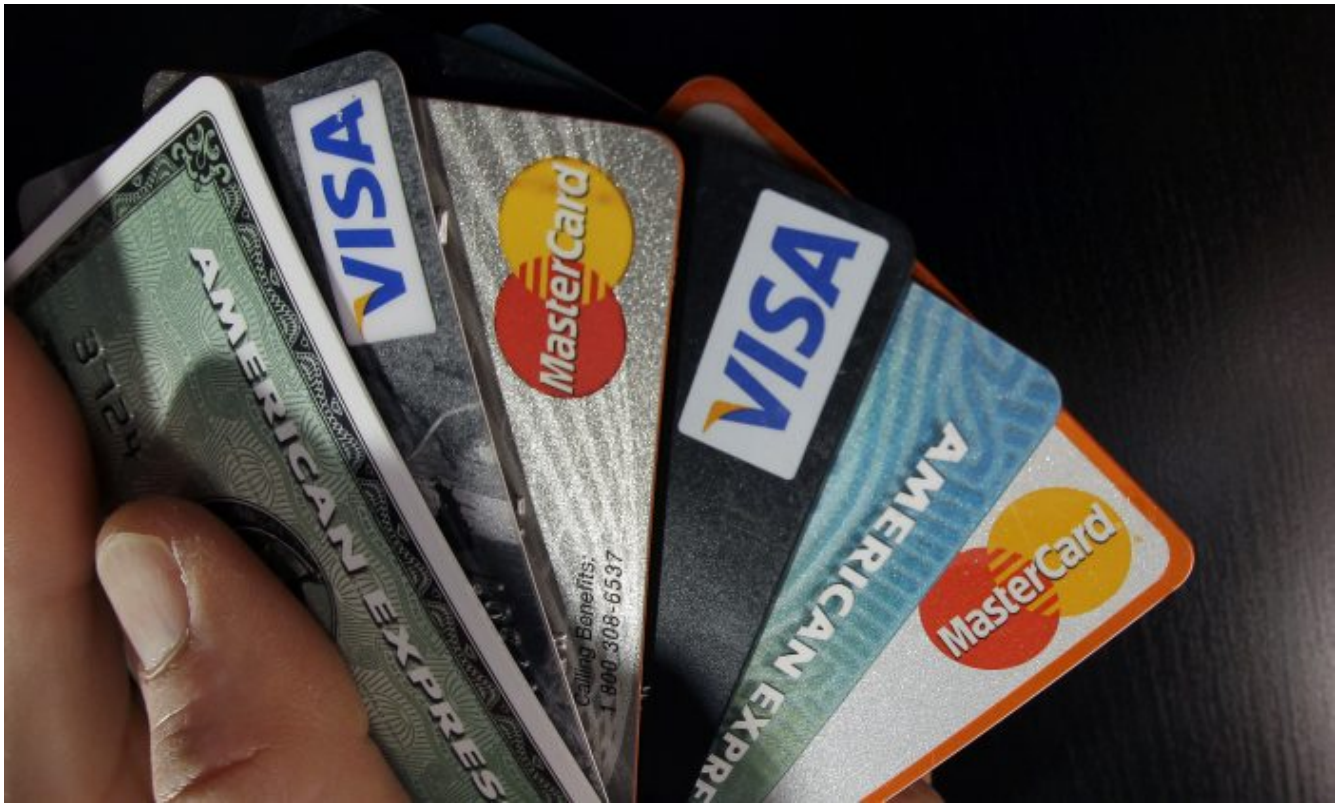
RED DRAGON MENACING

Chinese Communist Party(CCP) Exposed

NOVEMBER 10, 2021 BY ADMIN

513. No More China Tech: 57 Million Credit Card Machines Likely Compromised



Consumer credit cards are posed in North Andover, Mass., on March 5, 2012. (Elise Amendola/AP Photo)

No More China Tech: 57 Million Credit Card Machines Likely Compromised

Hundreds of millions of credit card users join Zoom and TikTok in likely data loss to China

Anders Corr

November 9, 2021 Updated: November 10, 2021

News Analysis

Americans and allies are too dependent on China tech, as demonstrated by recent revelations that our Chinese-manufactured credit card machines are sending data back to China for no good reason.

The U.S. Treasury Department says that millions of Chinese point-of-sale (POS) devices, the credit card machines found at check-out counters, could be sending customer data back to China for no good reason.

Treasury Department lab tests show that the data is encrypted and sent to unknown third parties in China. The transmissions are "superfluous to normal payment transaction processing," according to a letter from the Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP), as quoted in Bloomberg News. The China-bound data transmissions are larger and more frequent than the transmissions of normal payment transactions.

"Treasury's preliminary assessment is that data transmission by these devices indicates the possibility of risks to customer data confidentiality," a Treasury spokesperson emailed to Bloomberg.

A subsidiary of the Chinese company, PAX Global, claimed that the security concerns were just “rumors.” The company’s headquarters are split between Hong Kong and Shenzhen, China. PAX has manufactured 57 million terminals that operate in 120 countries around the world, according to its own claims.

Global Payments Inc., the credit card processing company that recently said it was subject to a massive security breach, announced on April 2 that around 1.5 million credit card numbers were exposed. (Chris Hondros/Getty Images)

On Oct. 26, the FBI raided PAX offices in Jacksonville, Florida. And two days later, the company’s senior vice president of security and services quit her job.

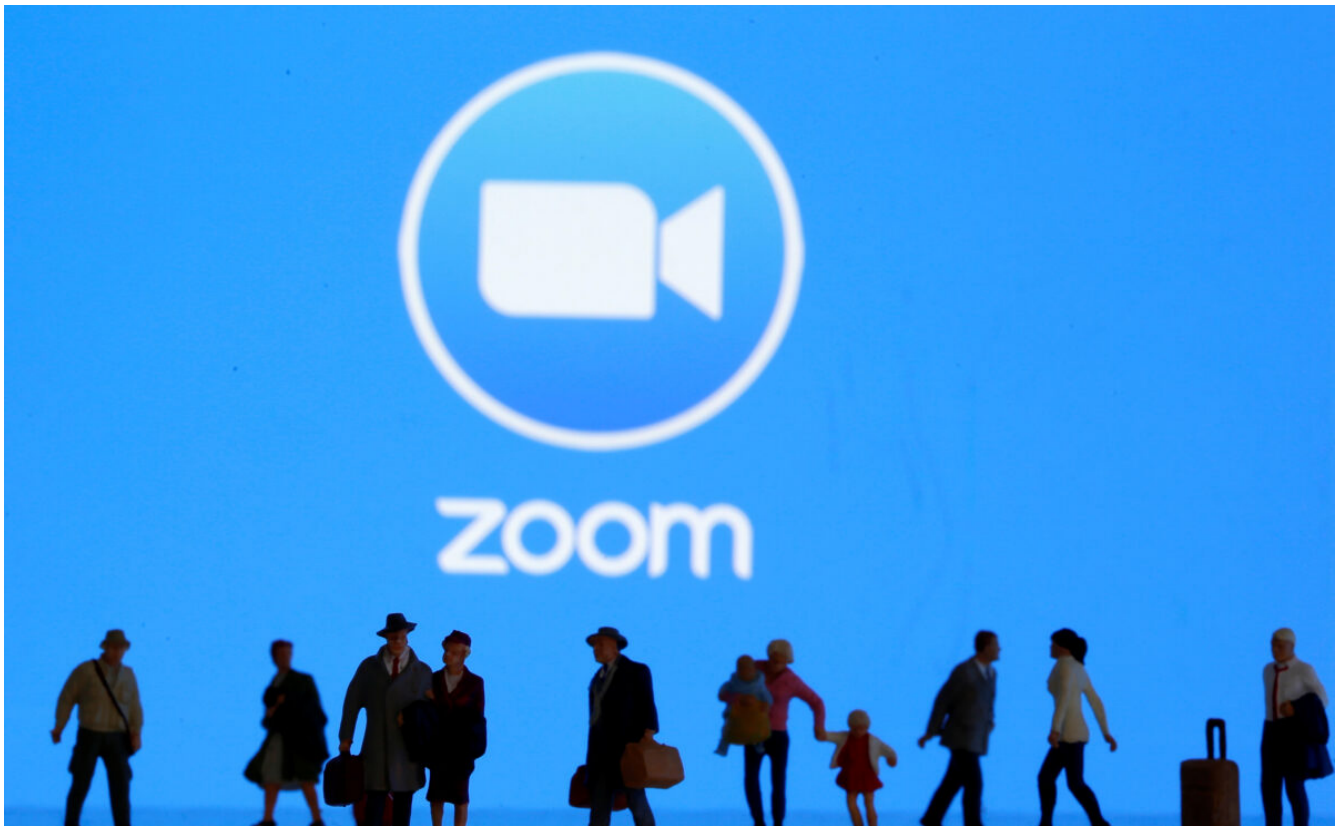
A British security agency is also investigating the Chinese POS device manufacturer.

Cybersecurity expert Brian Krebs reported that the FBI raid was not only linked to the discovery of "unusual network packets" from the company's terminals, but to reports that the PAX systems could be linked to cyberattacks, hacks, and illicit data collection on U.S. and European Union organizations.

Financial company FIS Worldpay, a Florida-based payment processing company, has for security reasons been forced to replace its PAX terminals with machines from American and French manufacturers. A FIS spokesman explained that the reason FIS is replacing PAX terminals is because FIS "did not receive satisfactory answers from PAX regarding its POS devices connecting to websites not listed in their supplied documentation."

The likely compromise of American and allied financial data by Chinese-manufactured POS credit card machines is the tip of the iceberg of vulnerability to China tech. Other China-linked companies, like Zoom, TikTok, and computer and cell phone manufacturers, have hundreds of millions of global users who are vulnerable to data loss to China.

Zoom was downloaded 485 million times in 2020, and continues to have serious security issues. In 2020, the FBI issued a security warning about Zoom, and the Department of Defense forbade its affiliates to use the video-conferencing application. Zoom's encryption keys were available to the Chinese regime, and its international meeting traffic routed through Chinese servers.



Small toy figures are displayed in front of a Zoom logo in this illustration taken on March 19, 2020. (Reuters/Dado Ruvic/Illustration)

Yet in 2020, 90,000 schools in 20 countries made the wrong decision and utilized Zoom. Skype and Google

provide better video calls, but the Zoom craze has gone dangerously viral.

The high rate of usage among naive Zoom users, many of whom are children, is not due to lack of warning.

“Zoom was found to be sending unauthorised data to Facebook,” according to a recent article in the Business of Apps. Its past hoarding of data and sub-standard encryption, identified by academic researchers, is well known. “Zoom saw itself banned by governments for official business (Canada and Taiwan), numerous organisations (SpaceX and Nasa) and school boards (New York and Taiwan),” according to the article.

As late as September 2021, Zoom software allowed remote code execution, that is, hacking of user machines over the internet. Zoom supposedly found and fixed the vulnerability, which is why we know about it. But with a lagging track record on security over the years, which is often only fixed when Zoom is caught with its hand in the digital cookie jar, who knows what remains. Prudence should be the order of the day. Stop using Zoom.

TikTok is even closer to China, and was downloaded 850 million times in 2020, and over three billion times overall. Twenty-eight percent of TikTok users are under the age of 18, and 59 percent are female. North America had 105 million users in 2020.

TikTok is owned by ByteDance, which is headquartered in Beijing.

Due to national security concerns, India banned the app in June 2020. Two months later, President Donald Trump signed an executive order requiring either the divestment of Bytedance from TikTok, or an American purchase of the app. However, the Biden administration unwisely revoked the order.

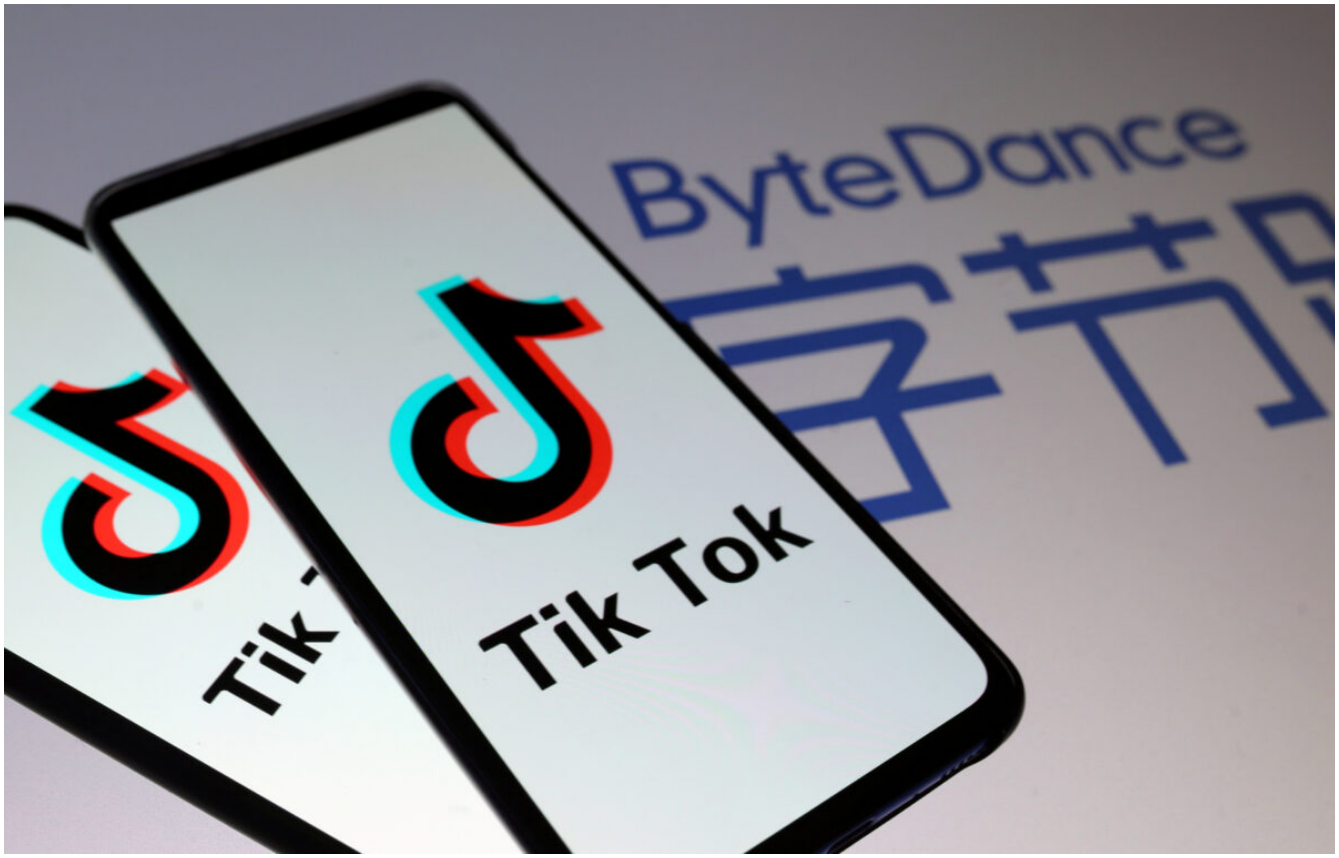
In April, the Beijing regime doubled down by taking a 1 percent stake in a key Bytedance management company, and one of its three board seats, according to The Information.

In response, Senator Marco Rubio (R-Fla.) rightly blasted the Biden administration, which he said "can no longer pretend that TikTok is not beholden to the Chinese Communist Party. Even before today, it was clear that TikTok

represented a serious threat to personal privacy and U.S. national security. Beijing's aggressiveness makes clear that the regime sees TikTok as an extension of the party-state, and the U.S. needs to treat it that way. President Biden must take immediate action to remove ByteDance and TikTok from the equation."

Rubio rightly went beyond just a whack-a-mole approach. "We must also establish a framework of standards that must be met before a high-risk, foreign-based app is allowed to operate on American telecommunications networks and devices," he said.

The problem is not only China-linked software, however, but also the American and allied dependence on China's manufacture of computers, tablets, and phones. Ninety percent of computers, and 70 percent of cell phones, are manufactured in China. All of this hardware, therefore, includes a higher level of security risk.



TikTok logos are seen on smartphones in front of a displayed ByteDance logo in a file illustration picture. (Dado Ruvic/Illustration/Reuters)

The world's electronic device manufacturing processes are largely controlled by the Chinese Communist Party, which has proven to be unscrupulous in its pursuit of power. We tend to ignore the attendant perils for reasons of convenience and budget, but we do so at our own grave risk.

The U.S. Treasury Department has hinted that technology from China should be rejected because of the higher risk it entails.

“OCCIP encourages stakeholders in the U.S. financial system to adopt a risk-based approach to protecting the confidentiality of their customers’ data, the integrity of their networks, and the availability of their services,” the Treasury Department said in this month’s letter about the PAX investigation. “Banks and financial service providers should apply this risk-based approach to their supply chains.”

While such warnings are welcome, they are entirely insufficient. We need laws and executive orders that mandate and provide for a fully secure technological environment for America and our allies. Our information security depends upon U.S. and allied control and protection of all information technology, from seed investment, to ownership, hardware manufacture, and the writing and operation of software that gives life to our networks. Nothing else will do.

It is unconscionable that U.S. and allied governments continue in their failure to protect our democratic communities from unscrupulous China-linked technology manufactures, including software like TikTok and hardware like computers, phones, and credit card machines, at the expense of American and allied privacy, workers, and the

diversity of our industrial ecosystems, and those of our allies.

Our democratic governments must get smart fast, or the loss to China will be irreversible, and ultimately entail the loss of democracy itself.

Anders Corr has a bachelor's/master's in political science from Yale University (2001) and a doctorate in government from Harvard University (2008). He is a principal at Corr Analytics Inc., publisher of the Journal of Political Risk, and has conducted extensive research in North America, Europe, and Asia. He authored "The Concentration of Power" (forthcoming in 2021) and "No Trespassing," and edited "Great Powers, Grand Strategies.

https://www.theepochtimes.com/no-more-china-tech-57-million-credit-card-machines-likely-compromised_4090346.html

COMMUNISM EXPOSED 2