Hit by a ransomware attack? Your payment may be deductible

June 19 2021, by Alan Suderman and Marcy Gordon

In this photo March 22, 2013, file photo, the exterior of the Internal Revenue Service (IRS) building in Washington. As ransomware attacks surge, the FBI is doubling down on its guidance to affected businesses: Don't pay the cybercriminals. But the U.S. government also offers a little-noticed incentive for those who do pay: The ransoms may be tax deductible. Credit: AP Photo/Susan Walsh, File

As ransomware attacks surge, the FBI is doubling down on its guidance to affected businesses: Don't pay the cybercriminals. But the U.S. government also offers a little-noticed incentive for those who do pay: The ransoms may be tax deductible.

The IRS offers no formal guidance on ransomware payments, but multiple tax experts interviewed by The Associated Press said deductions are usually allowed under law and established guidance. It's a "silver lining" to ransomware victims, as some tax lawyers and accountants put it.

But those looking to discourage payments are less sanguine. They fear the deduction is a potentially problematic incentive that could entice businesses to pay ransoms against the advice of law enforcement. At a minimum, they say, the deductibility sends a discordant message to businesses under duress.

"It seems a little incongruous to me," said New York Rep. John Katko, the top Republican on the House Committee on Homeland Security.

Deductibility is a piece of a bigger quandary stemming from the rise in ransomware attacks, in which cybercriminals scramble computer data and demand payment for unlocking the files. The government doesn't want payments that fund criminal gangs and could encourage more attacks. But failing to pay can have devastating consequences for businesses and potentially for the economy overall.

A ransomware attack on Colonial Pipeline last month led to gas shortages in parts of the United States. The company, which transports about 45% of fuel consumed on the East Coast, paid a ransom of 75 bitcoin—then valued at roughly $4.4 million. An attack on JBS SA, the world's largest meat processing company, threatened to disrupt food supplies. The company said it had paid the equivalent of $11 million to

hackers who broke into its computer system.

Ransomware has become a multibillion-dollar business, and the average payment was more than $310,000 last year, up 171% from 2019, according to Palo Alto Networks.

The companies that pay ransomware demands directly are well within their rights to claim a deduction, tax experts said. To be tax deductible, businesses expenses should be considered ordinary and necessary. Companies have long been able to deduct losses from more traditional crimes, such as robbery or embezzlement, and experts say ransomware payments are usually valid, too.

Colonial Pipeline CEO Joseph Blount testifies during a Senate Homeland Security and Government Affairs Committee hearing one day after the Justice

Department revealed it had recovered the majority of the $4.4 million ransom payment the company made in hopes of getting its system back online, Tuesday, June 8, 2021, on Capitol Hill, in Washington. Credit: Andrew Caballero-Reynolds/Pool via AP

"I would counsel a client to take a deduction for it," says Scott Harty, a corporate tax attorney with Alston & Bird. "It fits the definition of an ordinary and necessary expense."

Don Williamson, a tax professor at the Kogod School of Business at American University, wrote a paper about the tax consequences of ransomware payments in 2017. Since then, he said, the rise of ransomware attacks has only strengthened the case for the IRS to allow ransomware payments as tax deductions.

"It's becoming more common, so therefore it becomes more ordinary," he said.

That's all the more reason, critics say, to disallow ransomware payments as tax deductions.

"The cheaper we make it to pay that ransom, then the more incentives we're creating for companies to pay, and the more incentives we're creating for companies to pay, the more incentive we're creating for criminals to continue," said Josephine Wolff, a cybersecurity policy professor at the Fletcher School of Tufts University.

For years, ransomware was more of an economic nuisance than a major national threat. But attacks launched by foreign cybergangs out of reach of U.S. law enforcement have proliferated in scale over the past year and thrust the problem of ransomware onto the front pages.

In response, top U.S. law enforcement officials have urged companies not to meet ransomware demands.

"It is our policy, it is our guidance, from the FBI, that companies should not pay the ransom for a number of reasons," FBI Director Christopher Wray testified this month before Congress. That message was echoed at another hearing this week by Eric Goldstein, a top official at the Department of Homeland Security's Cybersecurity & Infrastructure Security Agency.

In this Oct. 12, 2020 file photo, a worker heads into the JBS meatpacking plant in Greeley, Colo. The world's largest meat processing company says it paid the equivalent of $11 million to hackers who broke into its computer system late last month. Brazil-based JBS SA said on May 31 that it was the victim of a ransomware attack, but Wednesday, June 9, 2021 was the first time the

company's U.S. division confirmed that it had paid the ransom. Credit: AP Photo/David Zalubowski, File

Officials warn that payments lead to more ransomware attacks. "We're in this boat we're in now because over the last several years people have paid the ransom," Stephen Nix, assistant to the special agent in charge at the U.S. Secret Service, said at a recent summit on cybersecurity.

It's unclear how many companies that pay ransomware payments avail themselves of the tax deductions. When asked at a congressional hearing whether the company would pursue a tax deduction for the payment, Colonial CEO Joseph Blount said he was unaware that was a possibility.

"Great question. I had no idea about that. Not aware of that at all," he said.

There are limits to the deduction. If the loss to the company is covered by cyber insurance—something that also is becoming more common—the company can't take a deduction for the payment that's made by the insurer.

The number of active cyber insurance policies jumped from 2.2 million to 3.6 million from 2016 to 2019, a 60% increase, according to a new report from the Government Accountability Office, Congress' auditing arm. Linked to that was a 50% increase in insurance premiums paid, from $2.1 billion to $3.1 billion.

The Biden administration has pledged to make curbing ransomware a priority in the wake of a series of high-profile intrusions and said it is reviewing the U.S. government's policies related to ransomware. It has not provided any detail about what changes, if any, it may make related

to the tax deductibility of ransomware.

"The IRS is aware of this and looking into it," said IRS spokesperson Robyn Walker.