Bloomberg BNA

Tax Management Memorandum™

Ransomware: Tax Compliance Issues for a New Reality

By Donald T. Williamson[*] and A. Blair Staley[**]

Companies are getting hacked more frequently but aren't disclosing the incidents in their regulatory filings, a trend that worries investors.[1]

****

[W]e're going to have to constantly evolve. The first computer viruses hit personal computers in the early 1980s, and essentially, we've been in a cyber arms race ever since. We design new defenses, and then hackers and criminals design new ways to penetrate them. Whether it's phishing or botnets, spyware or malware, and now **ransomware***, these attacks are getting more and more sophisticated every day. So we've got to be just as fast and flexible and nimble in constantly evolving our defenses.*[2] *(Remarks by former President Obama, emphasis supplied)*

****

One of the most difficult decisions that an organization has to make is whether or not to pay the attacker to gain access to encryption keys or the other methods to regain access to its data. . . . The decision to pay or not to pay [the ransom] should be considered by decision makers prior to an attack.[3]

INTRODUCTION

As former President Obama and the Wall Street Journal recently noted above, attacks on company computers are becoming rampant. Some 2,642 public and private companies were hacked in 2015, with companies paying over $86 billion in the same year for cyber protection that is expected to cost $94 billion in 2016.[4] ''Malware . . . infects computers and restricts users' access to their files or threatens the permanent destruction of their information unless a ransom . . . is paid,''[5] and, as the former president stated, corporate executives must react quietly and adroitly to these types of ransomware attacks.[6] This need for speed and flexibility means that decision makers must

[*] Professor Williamson, the Kogod Eminent Professor of Taxation and the Howard S. Dvorkin Faculty Fellow, teaches a number of subjects related to taxation, is director of the Masters of Science in Taxation degree program, and serves as executive director of the Kogod Tax Center. He served as Adjunct Professor of Law at American University's Washington College of Law. He previously served as senior manager for international taxation at the National Tax Practice Office of KPMG in Washington, D.C., and as Professor-in-Residence at KPMG's Washington office.

[**] Dr. A. Blair Staley, CPA MST, is a professor at Bloomsburg University of Pennsylvania, where he teaches tax and computer forensics and fraud examination. Prior to joining academe, Dr. Staley worked for the federal government, serving most recently as Accounting Officer and Director of Finance for the U.S. Patent and Trademark Office.

[1] Tatyana Shumsky, *When to Disclose You've Been Hacked*, The Wall Street Journal, September 20, 2016, at B5.

[2] Press Release, The White House, Remarks by the President at the Cybersecurity and Consumer Protection Summit (Feb. 13, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit.

[3] John P. Pironti, ''5 Key Considerations When Preparing for a Ransomware Incident,'' @ISACA Volume 7 (Apr. 6, 2016), http://www.isaca.org/About-ISACA/-ISACA-Newsletter/Pages/@-isaca-volume-7-6-april-2016.aspx?cid=edmi_1202040&Appeal=EDMi&sp_rid=MTE4MTI5NDg5MzQyS0&sp_mid=12832360#1.

[4] See Shumsky, above.

[5] Federal Bureau of Investigation, Ransomware on the Rise (Jan. 20, 2015) https://www.fbi.gov/news/stories/2015/january/ransomware-on-the-rise/ransomware-on-the-rise.

[6] Press Release, The White House, Remarks by the President at the Cybersecurity and Consumer Protection Summit (Feb. 13, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit.

plan in advance whether to pay ransom to regain access to their data, and if so, what should be the maximum payment a company would be willing to make. Similarly, to make such decisions in the best interest of the firm, organizations need to understand in advance the tax consequences, if any, of making ransomware payments.

This article discusses the basics of ransomware and explores tax planning and reporting issues associated with making ransom payments. The article also addresses the issue of whether ransomware payments constitute nondeductible illegal payments, deductible theft losses, or ordinary and necessary business expenses. It also discusses the tax consequences of such payments being made through a third party and offers suggestions to policy makers regarding the proper tax treatment of such payments.

WHAT IS RANSOMWARE?

Ransomware is an internet-based,[7] white-collar crime,[8] where a person's electronically stored data are seized or blocked by a third party who threatens its destruction but will release access to the information back to the victim only upon payment of a ransom.[9] Ransomware attacks most frequently occur when the victim or its employees leave unsecure data in their computers, e.g., over a weekend, to suddenly discover that access to the files and documents in every computer in the victim's business have been blocked. Typically, the victim then receives an email such as the one below declaring that all the firm's files have been encrypted and that a payment must be made to regain access to them.[10]

Too often, companies facing this hijacking make the decision to pay the ransom rather than attempt to remove the barrier by hiring computer experts — an expensive and time-consuming alternative — or calling the police to report a crime — an embarrassing public admission that confidential information has been stolen. Ideally, an organization may have cyber-insurance, which is offered by most major insurance companies, to provide protections against such attacks.[11] Organizations offering such insurance will almost always provide guidance and technical expertise on how to prevent such thefts.[12] Larger organizations also often have full-time cybersecurity professionals whose job is to recover and restore files using backup files stored at other locations. Because larger, more sophisticated enterprises have taken precautions against cyber attacks, hijackers more often aim their attacks upon smaller, more vulnerable victims that do not have the resources and expertise to block the malware or maintain backup files containing the seized data.[13]

Failing to have cyber insurance or the ability to independently recover or restore the files, organizations are faced with the unfortunate need to pay the hackers in the most expeditious and confidential manner possible. Frequently, organizations will make a risk-management decision to pay the ransom simply because it is more economical and operationally more efficient to pay the ransom to regain access to data rather than attempting to restore data to their computer systems by other means.[14]

Thus, despite the FBI and other enforcement agencies recommending that ransom not be paid,[15] businesses and individuals have conceded that they have

---

[7] Kevin V. Ryan & Mark L. Krotoski, *Avoid Undermining the Legitimate Needs of Law Enforcement to Solve Crimes Involving the Internet in Amending the Electronic Communications Privacy Act*, 47 U.S.F. L. Rev. 291, 293 (Dec. 1, 2012).

[8] Gerald Cliff & Christian Desilets, *White Collar Crime: What It Is and Where It's Going*, 28 Notre Dame J. L. Ethics & Pub. Pol'y 481 (2014).

[9] Federal Bureau of Investigation, Ransomware on the Rise (Jan. 20, 2015) https://www.fbi.gov/news/stories/2015/january/ransomware-on-the-rise/ransomware-on-the-rise.

[10] Anthony P. Valach, *What to do After a Ransomware Attack*, Risk Management, June 2016 at 12, 13, http://www.rmmagazine.com/2016/06/01/what-to-do-after-a-ransomware-attack/.

[11] Daniel Garrie & Michael Mann, *Cyber-Security Insurance: Navigating the Landscape of a Growing Field*, 31 J. Marshall J. Computer & Info. Tech. & Privacy L. 379 (2014).

[12] Valach at 12.

[13] *Id.*

[14] Pironti, at n. 3.

[15] Federal Bureau of Investigation, *New Internet Scam, 'Ransomware' Locks Computers, Demands Payment* (Aug. 9, 2012),

ISSN 0148-8295

no alternative but to pay if they wish to remain a going concern.[16] Because the thieves frequently demand payment not in any currency but in a nontraceable, tradeable commodity such as bitcoins, victims have difficulty acquiring the commodity and making payment within the few days usually demanded before the seized information will be made permanently encrypted. Therefore, in desperation, victims often reach out to a third party, often a computer security firm, with experience in these matters to assist in consummating the payoff.

With the ransom paid, the company then must face decisions regarding the proper treatment of the payment on its books and ultimately its tax return as a nondeductible illegal payment under §162(c)(2),[17] a deductible theft loss under §165(c), or even an ordinary or necessary trade or business expense under §162(a). The discussion below considers these alternatives.

RANSOMWARE CONSTITUTING AN ORDINARY AND NECESSARY BUSINESS EXPENSE

To be deductible under §162(a), a payment such as ransomware must be an ordinary and necessary business expense. Whether a payment qualifies for deduction under §162(a) is a factual issue that must be decided on the basis of all relevant facts and circumstances.[18]

For this purpose, the Supreme Court long ago found the meaning of ''ordinary'' to be that which is ''normal, usual and customary'' and therefore the expenditure is ''of the type which are common to, or frequently occur in the type of business in which [a taxpayer] is engaged.''[19] Given the pervasiveness of cyber attack on all types of businesses and the general concurrence of those attacked to pay off the perpetrators, a strong argument can be made that ransomware has become a normal, usual and customary expenditure for all types of businesses conducting transactions electronically.

Furthermore, because the determination of whether an expense is ''ordinary'' is ultimately a factual issue, the absolute number of taxpayers paying ransom in these circumstances is irrelevant. This is particularly important in that while cyber attacks are common, businesses are reluctant to disclose such payments so that the number of victims is simply unknown. Thus, a compelling argument can be made that ransomware payments are ordinary within the meaning of §162.

But in addition to being ordinary, to be deductible under §162 expenses also must be ''necessary,'' meaning that they are ''appropriate and helpful'' for ''the development of the taxpayer's business.''[20] In the case of ransomware, it is self-evident that such payments are appropriate and helpful. Most businesses will easily be able to establish that the information taken from them is essential to their continuation as a going concern and is needed to protect or enhance their business. In short, taxpayers have legitimate, even powerful, arguments for deducting ransomware payments as ordinary and necessary business expenses.

Finally, characterization of ransomware as being a capital expenditure is incorrect in that the payments do not constitute an investment in the business and are not creating an asset with either a definite or indefinite useful life that could produce added value in future years, but rather only result in the return of information that itself is not a capital asset.

RANSOMWARE CONSTITUTING A THEFT LOSS

As an alternative to a deduction under §162(a), §165(a) allows, with a few exceptions not relevant in this case, a deduction for any loss sustained during the taxable year that is not compensated for by insurance or some other means. Section 165(c) limits losses to those incurred in a trade or business, losses incurred in any transaction entered into for profit, and personal losses (subject to a $100 floor and 10% adjusted gross income threshold) incurred by individuals arising from ''fire, storm, shipwreck, or other casualty, or from theft.'' Judicial definitions of ''theft'' for the purposes of §165 include ''any criminal appropriation of another's property to the use of the taker, particularly including theft by swindling, false pretenses, and any other form of guile,''[21] or any ''illegal takings other than . . . larceny.''[22] The Internal Revenue Service defines theft to include an illegal taking of the taxpayer's property under state law with criminal intent with

---

https://www.fbi.gov/news/stories/2012/august/new-internet-scam/new-internet-scam.

[16] Valach at 12. *See also, e.g.,* Aarti Shahani, *Ransomware: When Hackers Lock Your Files, to Pay or Not to Pay?*, KDLG (Feb. 13, 2015), http://kdlg.org/post/ransomware-when-hackers-lock-your-files-pay-or-not-pay.

[17] Unless otherwise stated, all section references are to the Internal Revenue Code of 1986, as amended, and the regulations promulgated pursuant thereto.

[18] *Commissioner v. Heinger*, 320 U.S. 467, 473–475 (1943).

[19] *Deputy v. DuPont*, 308 U.S. 488, 495 (1940).

[20] *Commissioner v. Tellier*, 383 U.S. 687, 689 (1966).

[21] *Edwards v. Bromberg*, 232 F.2d 107, 110 (5th Cir. 1956).

[22] *Farcasanu v. Commissioner*, 436 F.2d 146 (D.C. Cir. 1970), *aff'g per curium* 50 T.C. 881 (1968).

ISSN 0148-8295

the purpose of the seizure by the perpetrator being to receive a ransom for its return.[23]

Applying this standard to kidnapping, the IRS has ruled that to be deductible, a ransom payment need not be an ordinary and necessary business expense, but simply constitute a payment connected with an illegal taking. Consequently, a ransom payment made in connection with kidnapping, a criminal act in most states, constitutes a deductible theft loss.[24]

> **Example 1:** Baby Jane Doe is kidnapped with criminal intent in a state where kidnapping is a crime. Her parents' payment of a ransom for her release is an itemized deduction under §165 subject to the $100 floor and 10% adjusted gross income limitation.
>
> **Example 2:** If, in the preceding example, the Vice President of Company X was kidnapped, the ransom paid by X would be fully deductible under §165(a).

Rather than kidnapping a person, the perpetrators of ransomware ''kidnap'' information demanding money in exchange for the release of information that is necessary, indeed probably essential, for the continuation of the victim's business. Even where the encryption is personal to the victim, as in the case of information on an individual's personal laptop, the ransom payment would constitute a personal casualty loss, although its deductibility would depend on whether the payment exceeded 10% of the individual's AGI.[25]

RANSOM DISTINGUISHED FROM ILLEGAL PAYMENTS

While judicial and administrative rulings allow ransom payments directly connected to kidnappings to be deductible under §165, illegal payments, even if otherwise ordinary and necessary business expenses, generally remain nondeductible under §162(c)(2) as follows:

> No deduction shall be allowed under subsection (a) for any payment * * * made, directly or indirectly, to any person, if the payment constitutes an illegal bribe, illegal kickback, or other illegal payment under any law of the United States, or under any law of a State (but only if such State law is generally *enforced*), which subjects the payor to a criminal penalty or the loss of license or privilege to engage in a trade or business. * * * The burden of proof in respect of the issue * * * as to whether a payment constitutes an illegal bribe, illegal kickback, or other illegal payment shall be upon the Secretary to the same extent as he bears the burden of proof under section 7454 (concerning the burden of proof when the issue relates to fraud). (Emphasis supplied)[26]

There are many cases where courts have denied the deductibility of payments found to be in violation of the law. For example, in *Frederick Steel Co. v. Commissioner*,[27] the Tax Court found that ''commissions'' paid to the purchasing agent of the company's largest customer were not usual and customary but rather were nondeductible illegal payments under a state law prohibiting ''graft,'' i.e. the acquisition of gain by means of abuse of one's position in government, business, or other position of influence. Similarly, in *John J. Wells, Inc. v. Commissioner*,[28] the Tax Court held that blackmail payments were not deductible, because they were not a customary practice in the taxpayer's business.

> **Example 3:** X, a sole proprietor and owner of a profitable business, pays a ''street tax'' of $200 a month to avoid having his business destroyed. Extortion is illegal in the state where X operates, and prosecution of those committing extortion is generally enforced. If X's payment violates a state or federal statute prohibiting X from making such payments, X may not deduct the payment.

Allowing a theft loss deduction for ransom paid in connection with a kidnapping in violation of state law is based upon the courts' broad interpretation of what constitutes ''theft'' under §165 coupled with a narrow reading of an illegal payment under §162(c)(2). Thus, courts will in general allow a deduction for payments that might be considered in furtherance of an illegal activity so long as they are not in direct violation of a statute and are not against sharply defined national policies, e.g., a policy against permitting deductions associated with the business of drug trafficking.[29]

---

[23] Rev. Rul. 72-112, 1972-1 C.B. 60.

[24] PLR 7946010.

[25] §165(c), §165(h).

[26] §162(e)(2) (emphasis supplied). Section 7454 provides that in any proceeding involving whether a taxpayer committed fraud, the burden of proof is upon the government.

[27] 42 T.C. 13 (1964), *rev'd and rem'd on another issue*, 375 F.2d 351 (6th Cir. 1967).

[28] T.C. Memo 1984-79.

[29] *Holt v. Commissioner*, 69 T.C. 75 (1977). In *Holt* a loss was

ISSN 0148-8295

For example, in *Brizell v. Commissioner*,[30] the Tax Court held that payments made by a printing company to purchasing agents were deductible as they were usual and customary in the printing industry and not prohibited by the state's commercial bribery laws.

> **Example 4:** X, a sole proprietor and owner of a profitable business, makes payments of $200 a month to owners of local suppliers to ensure continued patronage. In X's jurisdiction, such ''kickbacks'' are usual and customary and do not violate state commercial bribery laws and are not against sharply defined national policy. X may deduct the payment.

In short, if the payment of ransomware does not directly violate a statute prohibiting its payment and if it does not violate some defined national policy, it is deductible despite its indirect promotion of illegal activity of stealing or rendering useless the taxpayer's data.

RANSOMWARE PAYMENTS AS ILLEGAL PAYMENTS, DEDUCTIBLE EXPENSES, OR THEFT LOSSES — THREADING THE NEEDLE

Determining whether a payment violates some federal or state law unconnected with the Internal Revenue Code is usually beyond the expertise of most tax lawyers and certainly not within the purview of the authors of this article.[31] However, at least one court in applying New York's bribery statute found such payments to not fall under §162(c)(2) where the taxpayer's payments were not voluntary but rather extorted through fear.[32]

While no definitive law on the deductibility of ransomware payments has been found, private discussions with computer professionals and business persons victimized by hackers indicate that such payments are becoming usual and customary in the ordinary conduct of small and medium size businesses and certainly are necessary for a business to continue operations. Nevertheless, even if such payments constitute ordinary and necessary trade, business expenses, or deductible losses, they remain nondeductible if they violate federal or state laws.

> **Example 5:** X's computer systems were illegally seized on Sunday, rendering proprietary data inaccessible to X's owner and employees. When a ransom was demanded for the release of the data, X contacted local law enforcement officials who stated that the seizure constitutes a criminal act and that payment by X would constitute a criminal offense. On Monday, X nevertheless pays 200 bitcoins to have the computer system unencrypted. X may not deduct the value of the bitcoins as a theft loss or business expense.
>
> **Example 6:** The same as the preceding example except the police inform X that payment of the ransom is not a criminal act. X may deduct the payment.

These examples illustrate the interaction of §162(a), §162(c)(2) and §165 to ransomware payments, the deductibility of which turns upon answers to questions such as the following:

- Are the payments usual and customary or infrequent and rare?
- At the time of demand for ransom, has the data already been encrypted, or is there merely a threat of encryption?
- Is the encryption of another person's data illegal under a federal or state statute?
- Is the payment against a sharply defined national policy, e.g., a payment to a terrorist organization?
- Do police or other law enforcement authorities recommend paying or not paying the ransom?
- If the police recommend not paying the ransom is their position based on a statute or other authority finding the payment to be illegal?

Thus, two otherwise similar scenarios may result in strikingly unsimilar results, based upon the interpretation of local law regarding whether the payment of ransom constitutes an illegal act.

REPORTING AND TREATMENT OF DEDUCTIBLE RANSOMWARE PAYMENTS

When, after considering the facts and circumstances of the specific seizure under §162(a) and §165 and the legality of payment under §162(c)(2), a tax-

---

distinguished from an expense, and despite the inapplicability of §162(f), a deduction was denied because such payments were against sharply defined national policy, i.e., drug trafficking.

[30] 93 T.C. 151 (1989).

[31] States are beginning to address this issue. For example, California enacted SB 1137 effective January 1, 2017, making the installation of ransomware a felony in the form of an extortion. Cal Penal Code §530. Maryland House Bill 340, introduced February 2, 2017, would create a criminal offense pertaining to extortion conducted through unauthorized software (http://mgaleg.maryland.gov/2017rs/fnotes/bil_0000/hb0340.pdf).

[32] *Brizell v. Commissioner*, 93 T.C. 151 (1989).

ISSN 0148-8295

payer concludes ransom payments are deductible, a further complication arises in that the reporting of a deduction for a ransomware payment depends on the entity paying the ransom, i.e., sole proprietorship, partnership including LLCs, S corporation, or C corporation.

Where the taxpayer claims the payment as an ordinary and necessary trade or business expense, the deduction is simply claimed on the applicable return or form, i.e., Schedule C for individuals filing Form 1040, Form 1065 for partnerships and LLCs, Form 1120 for C corporations, and Form 1120S for S corporations. However, if the expenditure is treated as a loss the reporting becomes more complex.

> **Example 7:** (*Individual-Personal*) Alfa, an individual with $100,000 of AGI, makes a ransomware payment of $25,000 in connection with the seizure of data of his personal laptop. The payment is reported on Section A of Form 4684, showing the $100 per casualty reduction[33] and the $10,000 (10% × $100,000) reduction.[34] The resulting amount of $14,900 ($25,000 – $100 – $10,000) is brought forward to line 20 of the Schedule A (Itemized Deductions) but is not subject to reduction under the 3% cutback rule for itemized deductions where AGI exceeds a certain threshold.[35]
>
> **Example 8:** (*Individual-Business*) Bravo, an individual with $100,000 of business income, makes a trade or business ransomware payment of $25,000. The $25,000 payment is reported on Section B of Form 4684 and on line 14 of Bravo's Form 1040. The $25,000 loss would reduce the $100,000 business income to reduce his total income (line 22) and AGI.
>
> **Example 9:** (*Partnership*) Charlie, a partnership with $100,000 of ordinary business income, makes a trade or business ransomware payment of $25,000. The $25,000 payment is separately reported on Section B of Form 4684; line 14 of Form 4797, line 6 of the Form 1065; line 11 of Schedule K; and line 11 (in an amount according to the partnership loss sharing agreement) of each partner's Schedule K-1.
>
> **Example 10:** (*S Corporation*) Delta, an S Corporation with a single owner and $100,000 of ordinary business income, makes a trade or business ransomware payment of $25,000. The $25,000 payment is reported on Section B of Form 4684; line 14 on Form 4797, line 4 on Form 1120S; line 10 of the Schedule K; and line 10 of the owner's Schedule K-1.
>
> **Example 11:** (*C Corporation*) Echo, a C Corporation with $100,000 of taxable income, makes a trade or business ransomware payment of $25,000. The $25,000 payment is reported on Section B of Form 4684; line 14 on Form 4797, and line 9 of the Form 1120.

However, if the victim's ransomware payments are found under federal or local law to be illegal the entity or individual may neither deduct nor capitalize the payment and it becomes a permanent book to tax difference for financial accounting purposes.

PAYMENT THROUGH A THIRD PARTY

In anecdotal discussions with computer professionals, most small businesses that are hacked are apparently making ransom payments, usually by transferring bitcoins through a third party — typically a computer technology firm that can quickly acquire and transfer the bitcoin within the deadline demanded by the hacker. In such cases, the third party, being nothing more than an escrow agent, need not report the ransomware payment. As noted by the Tax Court:

> We would agree that a taxpayer need not treat as income moneys which he did not receive under a claim of right, which were not his to keep, and which he was required to transmit to someone else as a mere conduit.[36]

Of course, any fee earned by the third party to complete the transfer would be taxable income and deductible by the victim.

> **Example 12:** X agrees to pay ransom to obtain release of encrypted data. X contracts with Y, a technology consultant, to exchange dollars for bitcoin and transfer the property to the hacker. Y charges an additional $1,000 to make the payment, backup X's data, and strengthen X's computer security. X may deduct the dollar equivalent of the bitcoin as a loss under §162 or §165 and the $1,000 consulting services as an ordinary and necessary business expense under §162. Assuming

[33] §165(h)(1).

[34] §165(h)(2)(A)(i).

[35] §68(c).

[36] *Vetrano v. Commissioner*, T.C. Memo 2000-128.

ISSN 0148-8295

there is no change in the bitcoin value, Y will not recognize the receipt or disbursement of the ransomware payment but will recognize the $1,000 as consulting fee income.

Finally, because bitcoin is treated as property, the value of which varies over time, and not money, the party paying the ransom may have taxable gain or loss depending upon the cost to purchase the bitcoin and the amount of ransom the bitcoin satisfies.[37]

OTHER COMPLIANCE ISSUES

In addition to the tax treatment of the payment and its reporting on the victim's tax return, 48 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands, have enacted legislation requiring entities to notify individuals of security breaches of information involving personally identifiable information, such as a name combined with a social security number, a driver's license, or an account number.[38] There are additional reporting and disclosure issues for public companies, calling for disclosure of cybersecurity risks and cyber incidents, including but not limited to ransomware attacks.[39] For instance, companies that are required to file with the SEC are required to report information breaches if they have a material impact on the financial statements. However, determining the materiality of a breach is a judgment decision for which there are no definitive guidelines. While the accounting profession has for years discussed creating guidelines to assist in making these decisions, the risk of offering too much information in reporting each breach or too little information that fails to report a significant breach has paralyzed the process.[40]

Additionally, U.S. persons may be prohibited from doing business with entities in certain countries, for example North Korea,[41] a possible source of the recent WannaCry ransomware attack.[42]

Finally, depending on the period of time from the purchase of the bitcoin to the date the bitcoin is used to satisfy the ransom, the victim's bitcoin payment may result in a taxable capital gain or loss based upon the cost of the bitcoins used to satisfy the specific dollar amount of payment, regardless of whether the acquisition of the bitcoin was by a third party acting as an escrow agent.[43]

CONCLUSION AND RECOMMENDATIONS

Ransomware has become so rampant a problem that it was noticed even by the President of the United States.[44] Whether ransomware is deductible as a theft loss, a trade or business expense, or is a nondeductible illegal payment, its treatment ultimately is dependent on the fact and circumstances of each case.

Because of this uncertainty, organizations must plan in advance not only on whether they will make such payments, but also whether they will deduct them. To alleviate concern regarding the deductibility of ransomware, specific guidance is needed from Treasury, IRS, or Congress itself on how to account for its tax treatment.

---

[37] *See* Notice 2014-21, 2014-16 I.R.B. 938.

[38] Valach at 13; see Security Breach Notification Laws, National Conference of State Legislatures (Apr. 2, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[39] Securities and Exchange Commission, CF Disclosure Guidance: Topic No. 2, Cybersecurity (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[40] Tatyana Shumsky, *When to Disclose You've Been Hacked*, The Wall Street Journal, Sept. 20, 2016, at B5.

[41] Exec. Order No. 13,722, 81 Fed. Reg. 14,943, (Mar. 18, 2016).

[42] Nicole Perlroth, *More Evidence Points to North Korea in Ransomware Attack*, N.Y. Times, May 22, 2015, *at https://www.nytimes.com/2017/05/22/technology/north-korea-ransomware-attack.html*.

[43] Notice 2014-21, 2014-16 I.R.B. 938, Q&A 7.

[44] Press Release, The White House, Remarks by the President at the Cybersecurity and Consumer Protection Summit (Feb. 13, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit.

ISSN 0148-8295