REPORT FROM THE EOUST

Robert S. Gebhard, Executive Office for U.S. Trustee; Washington, D.C. and
Nancy J. Gargula, Office of the U.S. Trustee; Indianapolis, IN

Protecting Against the Risks of Cyber Fraud: What Case Trustees Should Know

As a chapter 7 trustee, imagine you are in a court hearing on a motion to sell an asset of the estate in one of your cases. As soon as your hearing concludes, you look at your cell phone and see a dozen missed phone calls and what is clearly a frantic text from your assistant that reads, "Call me ASAP!", and shows a picture of a blacked-out computer screen displaying an ominous message that says: "Oops, your files have been encrypted!" Would you know what to do?

Unfortunately, several panel trustees have been victimized by this type of ransomware attack, which is a growing area of concern in the world of cyber security. In this article, we will address two common cyber fraud threats—ransomware and business email account schemes—and provide you with information on what to do if you fall victim to an attack along with preemptive measures you can take to reduce the threat to your operations and estate assets.

Ransomware

Ransomware is a type of malicious software or malware that encrypts and prevents access to a computer's files. Typically, a message will appear on the computer indicating that its data has been encrypted. The perpetrator demands a ransom and, until such time as it is paid, holds the data—such as documents, databases, photos, videos, and other files—hostage. Often, the perpetrator demands that the ransom be paid with Bitcoin or other cryptocurrency within a short time frame and may pressure the victim further by threatening to destroy the data or make the data public. In some instances, even if the ransom is paid, the data is never released back to the victim.

Perpetrators have several ways to infect computers with ransomware. They may hack into a user's account by taking advantage of security weaknesses in popular software, obtain credentials to user accounts on "dark web" markets, or launch a phishing campaign with emails that appear to be from a trusted sender. The phishing emails can be aimed at unveiling the victim's confidential information, such as username and password, or include a malicious file or link that, when opened, deploys the ransomware.

Fortunately, the panel trustees who have fallen victim to a ransomware attack have been able to recover their chapter 7 case data from their software vendor. And, while they suffered no case-related financial losses, they did incur expenses to recover other data and documents not maintained by the software vendor (*e.g.,* trusteeship records and pleadings); to evaluate the risks of paying the ransom[1] as compared with the cost in time and money to reconstruct pleadings from court filings; and, importantly, to assess the security of their computer system and implement security recommendations. The trustees also expended considerable effort to file police reports, assess remediation measures for the possible loss or exposure of personally identifiable information (PII) and conferred regularly with the Office of the U.S. Trustee to provide updates and obtain guidance as needed.

Drawing on the experience of these attacks, here are some of the immediate steps you should take if you are the target of a ransomware attack. First, immediately notify the U.S. Trustee, the local FBI office,[2] local law enforcement, your software vendor, and your insurance carriers as appropriate. You may also want to file a report with the FBI's Internet Crime Complaint Center.[3] Second, with initial notifications completed and, based on what is known about the attack, you must promptly determine the appropriate course of action and the level of notification required under applicable law to those individuals whose PII may have been disclosed, the resources needed to address the breach, and any appropriate remedial actions. You will need to consider the nature of the lost data (operational or personal), the sensitivity of the data, the amount of data, the number of individuals affected, the likelihood the perpetrator can use the data or cause harm with it, the strength and effectiveness of security technologies protecting the data and the ability to mitigate the risk of harm, among other factors.[4] You should also continue to assess the sufficiency of the response and potential remediation as additional information is obtained.

Business Email Compromise (BEC)

A business email compromise, also known as an email account compromise, exploits the reliance of individuals on email for personal and professional purposes. According to the FBI, it is one of the most financially damaging online crimes.[5] BECs are generally aimed at getting individuals to transfer funds in response to what appear to be legitimate emails from trusted sources or to otherwise modify procedures for making payments. Anyone who handles transfers of funds may be a target of such schemes, including an individual who receives instructions on how to wire transfer funds

About the Authors

Robert S. Gebhard is the Assistant Director for Oversight in the Executive Office for U.S. Trustees in Washington, DC.

Nancy J. Gargula is the U.S. Trustee for Regions 10 and 21 and is based in Indianapolis, IN.

to a title company for the purchase of real estate or a business that is asked to change the bank account number of a vendor. In bankruptcy cases, the email compromise schemes may target trustees who receive and disburse funds in connection with the administration of assigned cases.

A BEC perpetrator may attempt to hack into a computer system, send a phishing email, or spoof an email account or website by changing as little as one letter in a legitimate email address to trick the victim into thinking the email is from a known source. There have been a number of BEC attempts against bankruptcy trustees. Banks and vendors used by trustees can be targets too, which not only impacts the trustees but can harm the estates they administer. For example, in one instance a hacker accessed a bank employee's email account that in turn provided access to trustee account numbers, addresses, and case numbers and names for various bankruptcy estates.

In May 2020, the U.S. Trustee Program issued a notice to chapter 7, 12 and 13 trustees regarding email compromise schemes[6] after a bankruptcy law firm fell victim to a BEC scheme that resulted in a loss. In that matter, the perpetrator hacked into the law firm's computer system and created email rules to divert certain emails from an employee's account into a subfolder the hacker created. The perpetrator used the emails to redirect debtor payments intended for a chapter 13 trustee and a chapter 7 trustee by falsely telling the debtors that the trustees had moved to electronic payments through Venmo and PayPal. After clients confirmed they had accounts on these platforms, the perpetrator provided links to the bogus trustee accounts. When the chapter 7 trustee detected the scheme—after one of the debtors contacted the trustee about the electronic payment to be made—the trustee immediately notified counsel and the U.S. Trustee. The law firm also alerted the U.S. Trustee and provided information about the incursion.

Detecting Email Compromise Schemes

In a trustee's office, a BEC scheme may not come to light until missing payments are identified either by the trustee or are reported by a debtor or other third party and there is confirmation that the payments were misdirected. This underscores the need for trustees to maintain and update their internal controls and to look for irregularities in the banking process or in disbursement or payment transactions. In addition, constant awareness and diligence by trustees and the staff who assist them are needed to thwart phishing attempts. Emails requesting immediate action on or seek to change a form of payment or replace an account number should be scrutinized.

It is critical that you educate your staff about the risks of BEC and discuss ways to avoid putting the trustee operation at risk, including such common sense things as: (1) not posting any information about the work of the trustee's office on social media; (2) not clicking on links or files in unsolicited emails or text messages asking for updated payment or routing information; (3) carefully examining email addresses and URLs to ensure they are correct; (4) following policies on what can and cannot be downloaded on office computers; (5) being careful with emails that are forwarded with links or attachments; and (6) never emailing wire transfer or electronic payment instructions or acting upon them without first verifying the identity of the sender by phone or in person.

Responding to Email Compromise Schemes

If your trustee operation is affected by an email compromise scheme, you should immediately notify the U.S. Trustee and contact the bank where your bankruptcy estate funds are held to request that they contact the financial institution where the funds were sent, if known. You also should (1) notify your software vendor, local law enforcement and local FBI field office to report the crime (and may want to file a complaint with the FBI's Internet Crime Complaint Center); (2) contact your insurance carrier, if appropriate, to file a claim and take whatever other appropriate measures are necessary to recover the funds; and (3) if it is determined that there was a potential or actual a loss of data and PII, promptly determine the appropriate course of action and the level of notification required under applicable law to those individuals whose PII may have been disclosed, the resources needed to address the issues and appropriate remedial actions.

BEC Case Examples

- In December 2020, a chapter 7 trustee received an email purportedly from his attorney that made a change to wire transfer instructions previously provided. The trustee had just sent the instructions to his attorney and a hacker sent a reply impersonating the attorney. The trustee phoned the attorney and confirmed that the attorney did not send the email.
- In June 2019, a fraudster attempted to divert $3 million in estate funds that were being sent to the trustee from the court registry. The trustee had emailed the wire transfer instructions to the clerk. The court wired the funds to the correct account and the bank called the trustee to confirm receipt of the funds. A couple of days later, the bank called the trustee because the court clerk had received an email that appeared to be from the trustee indicating the transfer was sent to the wrong bank and was urgently requesting that the funds be recaptured and sent to the "correct" account. The fraudster, not the trustee, had sent the email, changing just one letter in the trustee's true email address.
- In July 2017, a chapter 7 trustee's assistant received an email from a hacker posing as the trustee and asked her to process a wire transfer. The assistant replied to the email, "Don't we need to get permission from the OUST first?" There was no specific reply to this question, but after more back and forth, the assistant realized it was a fraud. Again, the hacker had changed just one letter in the email address. A second attempt was made in May 2019 in the same office to intercept a wire transfer coming to the chapter 7 trustee. It too was thwarted.

Reducing the Threat of Cyber Fraud

Although cyber fraud is not a new problem, the pandemic and the move to a higher percentage of employees working remotely has greatly increased the risk

continued on next page

of becoming a victim of a cyber fraud. Accordingly, it is recommended that all trustees take the following steps to help minimize the threat of harm.

1. Keep all operating systems, web browsers, software and other applications current. It is also important to use up-to-date antivirus software.

2. Follow password best practices, such as never revealing passwords to others, using different passwords for different accounts, utilizing lengthy and complex passwords, using multi-factor authentication wherever possible and considering utilizing a password manager (already available on Android and Apple devices).

3. Immediately report all cyber incidents. Whether you see a potential threat or are a victim, chances are you are not the only one at risk and reporting the incident quickly may prevent the perpetrator from harming others.

4. Regularly backup data, systems, images and configurations, to include important documents, emails or data not regularly backed up by your software provider. Keep in mind that only certain data can be reconstructed through the trustee's software vendor.

5. Make certain all security solutions are up to date and regularly assess the adequacy of your system's firewalls. Consider whether cyber fraud insurance is needed or whether limits on existing policies need adjustment.

6. When updating your Continuity of Operations Plan (COOP) consider including specific measures to respond to cyber intrusions, such as steps to take and contact information in the event of an incident. It may also be helpful to identify one or two IT firms that may be able to assist in addressing cyber intrusions and include that contact information in the COOP.

7. When sending estate funds by electronic transfer, never email wire transfer instructions or other electronic payment information due to of the risk of interception and misappropriation. Speak personally with the representative at the financial institution to convey wire instructions and to confirm the accurate completion of a wire or electronic transfer of payments. Also require the financial institution to speak with the trustee personally to confirm requests to change previously provided instructions. Finally, if a trustee receives a request purportedly from a known third party to change previously provided electronic payment or wire transfer instructions, speak with them personally to confirm.

Conclusion

As with technology itself, cyber perpetrators continue to evolve in their methods of cyber intrusion and fraud. By taking the measures noted above, trustees can minimize risks to their computer systems and to bankruptcy cases under their administration. And by being vigilant, promptly reporting compromises and sharing information as new cyber fraud threats emerge, the U.S. Trustee Program and the chapter 7 trustees can continue to actively combat cyber fraud that could negatively impact the bankruptcy system.

Suzanne Hazard, Deputy Assistant Director, Chapter 7 Oversight, contributed to this article.

ENDNOTES:

[1] "The FBI does not support paying a ransom in response to a ransomware attack." *See* https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware.

[2] *See* https://www.fbi.gov/contact-us/field-offices.

[3] *See* https://www.ic3.gov/default.aspx.

[4] *See Handbook for Chapter 7 Trustees*, pages 5-22 to 5-23.

[5] *See* https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise.

[6] *Notice to Chapter 7, Chapter 12 and Chapter 13 Trustees Regarding Email Compromise Schemes*, United States Trustee Program (May 5, 2020), distributed to trustees via email.