2018 CLM Annual Conference
March 14-16, 2018
Houston, TX

The Impact of Cyber Attacks and Data Breach Events on Professionals

Prevention and Reporting in the Event of a Data Breach

I. FACTS

A twenty person law firm in a medium sized city has an integrated business practice. The transactional practice includes commercial tax, corporate and real estate work with some personal services provided for business owners. The litigation group services the same clientele in litigation matters and also represents banks and other financial institutions in commercial litigation.

The firm maintains its own servers and leases various scanners, copiers, and on site computer equipment and devices. The firm supplies lap tops and provides a monthly allowance for attorneys for personal "bring your own" communication devices. The firm maintains all client files and its email exchange server on its network.

Attorneys can obtain access to both their firm emails and document by using their attorney identification number and an assigned password which they must change every six months. The firm did not employ a virtual private network (VPN) remote access system. The firm did not adopt a data breach response protocol and as such had no standing relationships with an outside IT support vendor to assist with such a plan

An attorney at the firm was attending a CLM conference in Houston and used the hotel's Wi-Fi system to log on to the firm server to revise a pleading and check her emails. Hackers set up a fake guest look alike Wi-Fi system and misdirected her to their site. Her sign in credentials and password were intercepted by a hacker during this session.

The stolen credentials allowed the hacker to enter the firm's network and enable a ransomware program which locked down and denied all users access to the firm's electronic records. The managing partner received an email demanding the payment of a payment in Bitcoin equivalent to $500,000 to free up the files.

Without a standing relationship with IT consulting firm, several days were lost while the firm searched for assistance. The IT firm assured the law firm that it could work around the malicious program and could recover the firm's records. However, once recovery efforts began, it was discovered the hacker also corrupted the firm's back-up system so that the data could not be recovered.

Frustrated by the period of delay, the hacker suspended negotiations. A week later the hacker reappeared doubling its demand. When communications resumed there were additional delays because the firm was only allowed to purchase two Bitcoins per day as a new user. In addition, after payment was made the firm's IT vendor determined the decryption tools were invalid. Valid decryption tools were only communicated in exchange for additional ransom payments of Bitcoin.

By the time the ransom was paid a period of one month had passed. Client asset purchases and sales were delayed including real estate closings. The litigation section was forced to postpone important hearings and discovery. Several clients sought and received fee refunds. Some clients terminated their relationship with the firm. After investigating all costs and lost business associated with the loss of service, the firm determined it had at least $800,000 in losses.

The IT firm indicated that it was it was highly unlikely that while inaccessible client records and confidential communications had been reviewed by the hacker, copied or accessed by third parties.

The law firm tendered its business interruption claim to its insurance carrier. Whereas the policy provided business interruption coverage, the policy had a Computers and Media Endorsement that limited coverage for physical loss and recovery of data including damage to data caused by a computer virus to $20,000. The carrier paid $10,000 and declined to pay additional loss.

II. QUESTIONS

1. Did the firm violate Model Rule 1.1 on competence by failing to implement a VPN two factor remote access system and/or a breach preparedness plan? How does Model Rule 1.6 respecting the duty to maintain client confidentiality impact that question?

2. Does it matter that the same result could have been achieved by sending a professional a spoofed realistic phishing email with an attachment containing an encrypted ransomware virus?

3. Would the answers be materially different in the case of a CPA or an insurance professional in light of AICPA and NAIC guidance respectively? Do state shine the light laws essentially require a response plan to comply given the standard notice and content deadlines?

4. The firm only notified clients with active files that were directly affected by the breach to the extent it impacted open engagements. However, based on the It vendor's assurances that the breach were likely contained, breach notices were not provided to other clients and third

parties. Did the firm comply with Model Rule 1.4 and state "shine the light' laws by failing to provide broader disclosure?

5. Should the firm's business interruption coverage apply notwithstanding the exclusion in light of the fact that the data was never lost but only held for ransom? In either case are there better products to avoid or mitigate the loss?

AN ACCOUNTANT'S DATA BREACH LIABILITY RISKS

Anatomy of a Tax Fraud Scheme

I. BACKGROUND ON HISTORY OF TAX PREPARER RELATED IDENTITY THEFT

Certified Public Accountants communicate directly with government agencies on more fronts than many professionals. Examples include preparation of audits and reviews filed with the SEC pursuant Electronic Data Gathering and Retrieval (EDGAR) system and the electronic tax filing system that accountants use via his Paid Preparer Tax Identification Number (PTIN).

The PTIN electronic filing system has been plagued by identity theft problems since it was first initiated. With great embarrassment, the IRS itself was forced to shut down its "Get Transcript" program in 2015. The program allowed a preparer or taxpayer to recover prior filings. The Service learned that hackers were stealing taxpayer information for use in fraudulent schemes. This included use of taxpayer information to commit identity theft in financial transactions as well as the filing of false returns to generate fraudulent refunds. A class action brought on behalf of 330,000 affected taxpayers was brought and dismissed under the *Clapper* doctrine which requires proof of "injury in fact" to support Article III Standing. *Welborn v. IRS*, 218 F. Supp. 3d 64, 77-80 (D. D.C. 2016).

Tax preparers continue to use the Service's on line filing system. There are two safeguards available as checks against identity theft.

One is a two factor password system for use by preparers the Service is rolling out this year. The second is active client monitoring system on the "Additional Activities" site pursuant to which the accountant can check the status of filings under his PTIN. An accountant can log in with their PTIN at various intervals to check for suspicious activities. The IRS updates the Additional Activities page on a weekly basis.

II. FACTS

A mid-sized full service accounting firm provides audit, review and compilation services to a niche clientele of mid-sized public companies. Those clients have contractual provisions in their fee agreements requiring the firm to maintain electronic data security and response systems substantially the same as those set forth in AICPA System and Organization and Controls (SOC) for Cybersecurity. Several public company clients have cost shifting and/or liquidated damage provisions in the event of gross negligence in failing to implement such controls.

As part of its overall accountancy practice, the firm provides tax planning services to clients including private companies and high wealth individuals. Those clients' returns and associated client records include confidential and proprietary information on assets held and business relationships. This includes ownership interests in other private enterprises and trusts. Such relationships may be reflected in part in the clients' returns. However, the information is not generally a matter of public record.

Return preparation and filing is provided as an extension of the firm's "full service" relationship with its clients. Some of the employees charged have tax preparation backgrounds but are not IRS enrolled agents. Returns they prepare are reviewed by a partner and filed under that partner's PTIN page.

The firm files returns, extension requests and other filings electronically. Notwithstanding its state of the art security programs that apply to its internal information management systems, the firm has never implemented a system to actively monitoring its PTIN accounts. Nor has it yet adopted the two factor password system recently rolled out by the IRS.

The firm hired a new preparer. Ms. Badapple, whose resume showed she had an impressive record of prior preparer positions as a tax preparer. However, the firm conducted no criminal background check on Ms. Badapple. Had it done so it would have learned she had multiple convictions relating to the use of computers in identity theft schemes.

During the 2017 tax year Ms. Badapple forwarded private confidential records covering a number of clients to third parties. Ms. Badapple surreptitiously downloaded historic returns, draft returns and other sensitive data on a flash drive from the firm's document management system. She forwarded the flash drive to outside fraudsters who paid her for the information and promised to keep her identity secret. The ring created phony returns with the information and obtained fraudulent refunds before the clients' filed their genuine returns.

The scheme was not detected for over a month. When genuine returns were filed The IRS began sending notifications to the firm that returns had already been submitted for the client under CPA partner PTIN numbers. Clients were informed of the breach and Forms 14157 reporting the fraud were filed with the IRS.

The IRS estimated that $700,000 in false refunds had been diverted off shore before the scheme was detected through a forensic investigation. The investigation led back to Ms. Badapple's downloads. She was promptly arrested and confessed.

The clients ultimately faced no obstacle to filing their legitimate returns. However, the final destination of prior year returns and other firm records containing sensitive and confidential client financial information was never determined. In her plea agreement Ms. Badapple cooperated with authorities. However, Badapple asserted she had been dealing with offshore parties. Badapple had no reliable information on those who courted her or what became of the information she forwarded.

III. QUESTIONS

1. No client lost any money as a result of this fraud. After verified Forms 14157 were filed with the IRS, all clients filed their legitimate returns in the ordinary course.

2. As a general proposition, criminal activity is considered too deviant in nature to support the foreseeability requirements of duty. In addition, absent identifiable special damages, the Economic Loss Doctrine generally prohibits recovery based on mere negligence. Is there an exception to the *Clapper* "apprehension of future injury" doctrine relied on by the IRS itself in *Welborn*. See, *Stacy v HRB Tax Group, Inc.*, 516 Fed. Appx. 588 (6th Cir. 2013)?

3. Are the actual or liquidated damages provisions in the fee agreements with the public companies enforceable in light of the fact that there was no breach of any warranty as to the firm's own proprietary information security systems or response protocol? Instead, the firm merely failed to follow a "best practices" suggestion by the IRS that firms monitor PTIN accounts for suspicious activity.

4. Could the firm be vicariously liable for Ms. Badapple's conduct under the Computer Fraud and Abuse Act (CFAA) 18 USC § 1030?

5. Could the firm be liable to the IRS under 26 § 301.7026.1 (reckless unauthorized disclosures in connection with preparation of return) or 26 § 6713 (monetary penalties for unauthorized use of taxpayer information in connection with return preparation services)?

EVERYONE HAS BEEN DUPED

WHO BEARS THE LOSS?

I. FACTS

An employment discrimination case was filed by an employee of a national restaurant chain by a terminated employee. After a period of litigation the case is settled. The agreement provides that the employee withdraws his assertion that he is entitled to be reinstated to his position. The settlement agreement calls for separate payments. One is for lost wages in the amount of $2,000. The second payment of $63,000 is characterized as compensatory damages. The $2,000 is to be paid to the employee directly by the employer and reflected as W-2 wages. The remaining $63,000 will be paid as compensatory damages with the stipulation that the employer file a Form 1099 in connection with this part of the settlement.

The settlement agreement stipulated that the Magistrate Judge who presided over the settlement negotiations shall have authority to resolve and disputes arising out of the settlement agreement.

After the settlement was reached the employer mailed the final wage check to the plaintiff in accordance with the settlement agreement. The settlement agreement provides that the full $65,000 shall be paid as consideration for the release but fails to specify the exact form of payment. The agreement merely states that the case will be dismissed within 15 days of payment.

After the wage check is sent the employee begins to exhibit signs of cold feet. He now insists he must have the $63,000 immediately under threat of refusing to go through with the settlement. The plaintiff's counsel alerts defense counsel to the problem. In response the defense counsel agreed to send the $63,000 check directly to the employee's residence via overnight courier. The necessary information on the employee's home address was provided to defense counsel via an email from the plaintiff's counsel on the day of this conversation.

Unbeknownst to defense counsel, during the period after the settlement was reached plaintiff's counsel received a series of emails, ostensibly from his client/employee directing that the settlement payment be directed to a bank in London. Suspicious of the emails the plaintiff's attorney called the client who verified that the client had not sent the emails. The attorney deleted the emails in conformity with ABA Guidelines he had read advising that such emails were designed to implant malware, should be deleted and that the attachments should not be opened.

Thereafter the hacker that the plaintiff's attorney had ignored apparently created a spoofed email account. The appearance and address closely resembled that of the plaintiff's attorney. From this address the fraudster communicated instructions that the funds be wired to the same unauthorized account in London. Knowing of the urgency of the demand for payment defense counsel believed the employee had changed his mind and sought a wire transfer.

Without contacting plaintiff's counsel to confirm the change of plans, defense counsel followed the directive and wired the funds to London as directed.

In fact, the only legitimate email from opposing/plaintiff's counsel directed that a check be sent to the client's residence.

II. QUESTIONS

In *Bile v RREMC, LLC*, 2016 LEXIS 113874 (E.D. Va 8/24/16) the court was required to determine whether the wire transfer of the settlement proceeds to the fraudster's account in London legitimately constituted payment under the settlement agreement. The Plaintiff made the obvious and logical argument that the payment requirement of the release was absolute. That a third party had deceived the employer's defense counsel to wire funds to a fraudster, instead of delivering a check to the client, was not a risk that should be placed on the employee plaintiff.

The employer argued that, unlike defense counsel, plaintiff's counsel was aware that a third party interloper had contacted plaintiff's counsel with fraudulent wire instructions. Plaintiff's counsel never advised opposing counsel that he had detected and foiled this fraud. As such defense counsel was not on notice to look out for a similar effort to misdirect the funds.

Without clear governing authority under Virginia law, the court turned to the law of commercial paper. The court held that, in the event of a misdirected payment, the payee or its agents are in the best position to avoid the loss. The plaintiff and his lawyer knew that a fraudster was attempting to misdirect the funds and had spoofed the client's email credentials. For that reason the court reasoned the plaintiff's lawyer was in the best position to tip off defense counsel that a wrongdoer was trying to misdirect the funds. The district court affirmed the magistrate judge's ruling that, though misdirected to an unauthorized party, the wire transfer satisfied the payment obligations of the settlement agreement.

By comparison, in *Lizjan v Sahn Ward Coschingano & Baker, PLLC* , 2012 N.Y. Misc LEXIS 6783 (8/7/12) the court held that apparent authority of an agent to direct settlement proceeds via wire transfer at a minimum raised a triable issue of fact as to apparent and actual authority. The court held that there was a reasonable dispute as to whether the defendant could rely on instructions at variance with the specific party identified to receive payment in the settlement agreement. This was so notwithstanding there was an agency relationship between the payee and the party that directed change in payment terms. However, the specific extent of the agent's authority had never been verified by counsel for the party with the payment obligation.

1. Which decision is correct? Does defense counsel have the right to rely on a fraudulent directive from an impostor to satisfy the terms of a release? Alternatively should the defendant have a duty to investigate conflicting instructions and obtain revised instructions signed by the actual claimant/payee on the manner of payment?

2. Given that the hoax arguably did not involve the negligent performance of specific legal work or involve a compromise of either party's computer system, would professional liability or commercial crime insurance cover the loss? See, *Taylor & Lieberman v Federal Ins. Co.*, 681 Fed Appx. 627 (9th Cir. 2/13/17).