New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 258—NO. 66
WEDNESDAY, OCTOBER 4, 2017

Outside Counsel

Expert Analysis

1st Dept. Sustains Claims Against Fund Administrator After Hackers Grab Millions

A legal feud is currently playing out in New York state court between the world's biggest hedge fund administrator and a former client, and it all started with an email from an address containing a single extra letter. At the center of the lawsuit is the question of responsibility for an email scam that resulted in hackers stealing millions in client funds, and it is a case study in the mounting problem of cyber wire fraud and allocating fault when funds go missing.

In March 2016, Tillage Commodities Fund, L.P., then a $10 million commodities investment fund, hired SS&C Technologies as its third-party fund administrator. As is typically the case, SS&C was responsible for executing wire transfers related to the fund's ongoing business operations such as investor redemptions, distributions, and expense payments.

By **Craig A. Newman**

And **Maren J. Messing**

In its 25-page complaint, Tillage alleges that, over a 21-day period last March, a series of fraudulent emails were sent to SS&C—purportedly from Tillage—requesting that money be transferred from the fund's account to a bank in Hong Kong. But the complaint charges that the fraudulent emails actually came from a domain name that included an extra "l" in the Tillage name (@tilllagecapital.com), a detail it says SS&C failed to notice.

Tillage's complaint then sets forth a laundry list of "red flags" that SS&C allegedly failed to notice: the emails sought the transfer of millions of dollars at a clip and contained grammatical errors which Tillage claims were not only inconsistent with prior Tillage communications but rendered them "unclear in substance," requiring SS&C to respond to the hackers with clarifying questions. Tillage also alleges that SS&C was dilatory and negligent following the transfers, failing to immediately notify Tillage of the incident and refusing to turn over copies of its email exchanges with the hackers.

At the outset of the case, SS&C moved to dismiss, seeking protection from a clause in its services agreement with Tillage that limits SS&C's obligations to damages "resulting from the gross negligence, willful misconduct, fraud, or bad faith of SS&C." The trial court judge, Hon. Barry R. Ostrager, refused to dismiss the breach of contract claim, noting that gross negligence is typically a question of fact and does not require a showing of intentional wrongdoing. *See Tillage Commodities Fund, L.P. v SS&C Tech.*, 2016 N.Y. Misc. LEXIS 4834 (Dec. 22, 2016). Judge Ostrager also allowed Tillage to move forward with a breach of implied covenant claim.

On appeal, the court largely sided with Tillage and permitted several claims to proceed. See Tillage Commodities Fund, L.P., v. SS&C Technologies, 151 A.D. 3d 607 (1st Dept. 2017).

CRAIG A. NEWMAN *is a partner at Patterson Belknap Webb & Tyler in New York and chair of the firm's privacy and data security practice.* MAREN J. MESSING *is an associate in the firm's litigation department in New York.*

The three-judge panel of the New York Supreme Court, First Department, held that the breach of contract claim—based on "defendant's disbursement of funds without plaintiff's instruction of approval"—could proceed.

"Although the alleged unauthorized transfer of funds does not appear to have been intentional," observed the court, "plaintiff has sufficiently alleged that defendant's conduct 'evince[d] a reckless disregard' for plaintiff's rights insofar as it failed to comply with basic cybersecurity precautions and actively disregarded its own policies as well as obvious red flags." The appellate court also sustained the breach of implied covenant claim based on allegations that SS&C did not "immediately notify plaintiff of the fraud and filings a misleading policy report with the Hong Kong police … ."

And in a counter to Tillage's claims, SS&C filed its own lawsuit against the commodities fund, claiming it was Tillage that dropped the ball by "abdicating their core responsibilities … and enabl[ing] unknown criminals to obtain authentic credentials for the [f]und and go undetected while using those credentials to steal millions from the [f]und's coffers." In the complaint, SS&C claims that Tillage's lawsuit is merely a "bad-faith effort" to shift blame. *See SS&C Techs v. Tillage Commodities,* No. 654765/2016, Dkt. No. 40 (New York Supreme Ct. June 5, 2017). Tillage has filed papers to dismiss SS&C's third-party complaint, which is pending.

Most recently, on September 28th, the Commodity Futures Trading Commission (CFTC) joined the fray, settling charges against Tillage for failure to supervise its fund administrator's operation of its bank account containing commodity pool participants' funds under 17 C.F.R. §166.3 (2017). That provision requires CFTC registrants to "diligently supervise" the handling of all activities relating to its business. The CFTC found that Tillage had also "failed to develop and implement policies and procedures reasonably designed to detect unauthorized or fraudulent withdrawals … from the pool bank account." By consenting to the settlement, Tillage neither admitted nor denied any of the CFTC's findings.

> It all started with an email from an address containing a single extra letter.

ACH Wire Fraud

Incidents of ACH wire fraud similar to *Tillage* have surged in recent years. A recent alert from the FBI's Internet Crime Complaint Center notes that such incidents reported have doubled in the past year, rising in 2016 to 40,203 from 22,143 a year earlier. More than 50 percent of the victims were in the United States. And it's difficult to peg a number of losses due to wire fraud with annual global estimates ranging in the billions.

Yet, even with these eye-popping statistics, reported decisions discussing ACH wire fraud are sparse. Few victims of this kind of heist launch full-fledged lawsuits. In that way, the *Tillage* case seems to be an outlier. But there have been cases between financial institutions and their customers over which party should bear the risk of loss for wire transfers that get hijacked by a cybercriminal. For the most part, these cases have been brought under Article 4A of the Uniform Commercial Code, which looks at whether a bank has commercially reasonable security measures in place and acted in good faith in effecting the wire transfer.

'Experi-Metal'

In *Experi-Metal Inc. v. Comerica Bank,* 2011 U.S. Dist. LEXIS 62677, 2011 WL 2433383 (E.D. Mich. June 13, 2011), a Michigan District Court ruled in favor of the plaintiff for $561,399 in losses following a phishing attack. The court determined that Comerica "had not operated in good faith with respect to its online banking protections." In so finding, the court looked at the volume and frequency of the false payment orders, the overdraft created, the company's previous wire activity, the destinations and beneficiaries of the funds, and the bank's knowledge of prior and current phishing attempts. The court found that a bank dealing fairly with its customers would have detected and stopped the fraud earlier, particularly because the activity was so out of the ordinary and caused a major overdraft of the plaintiff's funds. Comerica later reportedly settled the matter after the Federal Financial Institutions Examination Council came out with new regulations

suggesting that many banks' security procedures were no longer considered effective.

'Patco Constr.'

A year later, in *Patco Constr. Co., Inc. v. People's United Bank,* a community bank authorized six apparently fraudulent withdrawals from an account held by Patco after the perpetrators correctly supplied Patco's customized answers to security questions. Although the bank's security system flagged each of these transactions as unusually "high-risk" because they were inconsistent with the timing, value, and geographic location of Patco's regular payment orders, the bank's security system did not notify its customer of this information and allowed the payments to go through.

On cross-motions for summary judgment, the district court held that the bank's security system was commercially reasonable and on that basis entered judgment in favor of the bank on the count of Article 4A of the UCC. *Patco Constr. Co. v. People's United Bank*, No. 09-cv-503, 2011 U.S. Dist. LEXIS 86169, 2011 WL 3420588 (D. Me. Aug. 4, 2011). The U.S. Court of Appeals for the First Circuit reversed, finding that "it was commercially unreasonable for [the bank's] security system to trigger nothing more than what was triggered in the event of a perfectly ordinary transaction" where the payment orders were "entirely uncharacteristic of Patco's ordinary transactions," *Patco Constr. Co. v. People's United Bank,* 684 F.3d 197, 213 (1st Cir. 2012). Central to the First Circuit's decision was the fact that the bank had previously decided to implement a system requiring a customer to answer security questions for any transaction for more than $1, which "greatly increases the risk that a fraudster … would be able to access the answers to a customer's challenge questions because it increases the frequency with which such information is entered through a user's keyboard." *Id.* at 211. Given the factual complexities of the case, the First Circuit suggested that the parties resolve the matter by agreement, which they did.

Cyber wire fraud isn't going away and the amounts at stake will likely only get higher. The failure to focus on the contractual undertakings and internal controls that come into play to allocate risk in the event of wire fraud or cybercrime won't be just a painful lesson but an expensive one as well.

'Choice Escrow'

And more recently, in *Choice Escrow & Land Title v. BancorpSouth Bank,* 2013 U.S. Dist. LEXIS 36746, 2013 WL 1121339 (W.D. Mo., March 18, 2013) the district court granted summary judgment to the bank after the plaintiff customer had previously declined the bank's offer to implement dual control [or double authentication such as requiring both a password and token-based validation] on wire transfers and to place daily transfer limits on its account. The court found that the bank's security protocols were commercially reasonable and that it had acted in good faith in accepting the wire transfer request. The Eighth Circuit noted that the customer "knew that dual control provided a reliable safeguard against Internet fraud, and it explicitly assumed the risks of a lesser procedure notwithstanding the relative ease with which it could have implemented dual control." *Choice Escrow & Land Title v. BancorpSouth Bank*, 754 F.3d 611, 622 (8th Cir. 2014). The Eighth Circuit also distinguished the case from *Experi-Metal* on the grounds that the payment order in *Choice* "was not so unusual that it should have raised eyebrows." *Id.* at 624.

Implications

No matter how the *Tillage* case turns out, there's a lesson here. And it's not just for fund administrators and their clients. Cyber wire fraud isn't going away and the amounts at stake will likely only get higher. The failure to focus on the contractual undertakings and internal controls that come into play to allocate risk in the event of wire fraud or cybercrime won't be just a painful lesson but an expensive one as well.

Reprinted with permission from the October 4, 2017 edition of the NEW YORK LAW JOURNAL © 2017 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382 or reprints@alm.com. # 070-10-17-04