SS&C Sued by Hedge Fund for Cyber Heist

OCTOBER 11, 2016 BY CHRIS KENTOURIS LEAVE A COMMENT

Was incompetence, gross negligence, collusion or a good faith mistake the reason operations executives from fund administrator SS&C Technologies authorized the transfer of almost US$6 million from a client's commodities fund to Chinese hackers?

That is the question readers of a lawsuit filed by hedge fund Tillage Commodities Fund against SS&C Technologies will likely be asking themselves based on the number and extent of the blunders committed by SS&C's investor services executives. That is if one believes the account given by Tillage at face value.

Tillage claims that the spoofing scam was so amateurish that it should have been caught immediately. Calling Tillage's allegations sensationalist, SS&C counters that the lawsuit is without merit and will fight it in court. SS&C is the parent of SS&C GlobeOp, which performs -fund administration services.

The commodities fund manager is suing the fund administrator in a New York court for more than US$10 million on the grounds it repeatedly ignored its own protocols and deceived clients into thinking it had sound technology to prevent a cybersecurity breach. The theft has forced the four-year old Tillage, which invests in exchange-listed commodities futures contracts, to shut down operations.

By Tillage's account, employees of SS&C Technologies authorized the release of funds multiple times in March 2016 after receiving several badly written emails from Chinese hackers for the funds. An employee, identified as investor services associate Tom Martocci, and his colleagues,enabled the theft of US$5.9 million to take place over a period of 21 days by accepting and even correcting poorly written emails that were flagged by SS&C's software as being problematic. The SS&C employees, alleges Tillage, never even bothered to verify the identity of either the originator or the beneficiary of the request for the wire transfer.

SS&C had the sole authority to disburse Tillage funds to process investor redemptions or withdrawals, pay authorized fund expenses and accept or move subscription funds to a prime broker. By SS&C's own rules, access to customer financials and information is "restricted and controlled by identification, authentication and authorization control processes that are based on least privilege, need-to-do and need-to-know purposes." Employees are supposed to monitor for business email scams by looking at all of the email fields such as to, cc, and from for signs of fraud or spoofing. SS&C also requires that four people — an investor services associate, an accounting contact, a department manager and a department director in sequential order — sign off on any requests for the transfer of funds from Tillage. They each must verify any fund transfers with an invoice in the case of an expense or redemption letters and instructions in the case of a redemption.

Had SS&C's employees followed even the basic rules, Tillage would never have lost close to US$6 million, alleges the hedge fund's filing. Tillage's lawsuit argues that the actions — or inactions — of SS&C's staff defy reason. Here are just three of the most glaring examples of SS&C's conduct that Tillage describes in its lawsuit to support its claim of SS&C's gross negligence:

Correcting Rejected Emails

In the first fraudulent email dated March 3, 2016, the Chinese hackers asked that funds be wired directly to a company called Haoran Technology in its account at Hangseng Bank in Hong Kong. According to Tillage, Tom Martocci and other SS&C employees corrected the details of the transaction adding HSBC Hong Kong as the correspondent bank and Hangseng Bank as the beneficiary bank. When those corrections didn't work and the wire was again rejected, the lawsuit says, SS&C contacted the scammers again who amended the instructions and asked that the funds wired be to a firm called "Away Technologies" via an account at HSBC Bank in Hong Kong. The subsequent requests were also amended the same way.

The language of the initial fraudulent request should have been enough to raise red flags, says Tillage. "Can you please process the attached International Business Establishment. We are funding Haoran Technology Limited. Please leave me a mail to confirm this and that the wire will go out today," it said.

Who would accept the validity of such a badly written instruction that it was rejected by SS&C's own filters in the first place, let alone correct it, argues Tillage. How about asking for redemption documentation or any information about the investors wanting the money? What about verifying the identify of the firm Away Technologies. A search of the Internet doesn't show up any firms with that name. Or how about contacting Tillage itself? Surprisingly, none of those preventative steps was taken and it is unclear why SS&C's employees would go to such lengths as to correct emails that were initially flagged as problematic by SS&C's own filters.

Neglecting Precedent:

Tillage made a total of over 210 requests to SS&C for wire transfers covering expenses over its four-year existance. The average amount of the wire transfers was for only US$3,567 and the largest was for US$12,410. The only other wire transfers that occurred outside of investor subscriptions and redemptions was for the heavily documented transfers of the fund's bank account from J.P. Morgan to First Republic and the switch the fund made from its original prime broker being J.P. Morgan to its new prime broker ADM Investor Services. By contrast, the fraudulent wire transfers asked for six and seven figure amounts. They never mentioned any investors or provided any supporting documentation of the reason for the wire transfer, as was Tillage's customary policy.

The fraudulent email requests also concluded with the sentence: If you require anything further, please do not hesitate to send me a mail. The phrasing did not conform with previous Tillage communications which always concluded with "Should [SS&C] require anything further please call Tillage at the following number."

The emails repeatedly misspelled the name of Tillage Capital, were syntactically incorrect, and often colloquial in nature. Over the course of the four-year services agreement with SS&C, the domain name of Tillage Capital was tillagecapital.com while the fraudulent emails used a domain name with an additional l — tillagecapital.com. Not only was the language used in the first request suspicious, but so was the text used in the others. One email asking for the largest amount of monies — US$3 million — said nothing more than "How was your weekend? Let's round up business today."

Last, but not least, the requests to transfer funds to technology companies with bank accounts in Hong Kong did not match any Tillage's previous correspondence with SS&C. No one had ever requested any funds be transferred to Hong Kong.

According to Tillage, Martocci had received 40 legitimate wire transfer requests from Tillage prior to the fraudulent ones. Tillage argues that he sound have noticed the discrepancies between the previous correct and new fake ones.

Ignoring Basic Procedures

Tillage alleges that SS&C's employees didn't do anything that would have immediately alerted SS&C's management and Tillage of the cybersecurity breach. Contrary to SS&C's policy, the employees did not push a secure send button before wiring the funds. If they had Tillage would have been notified of the wire transfer and the spoofing would have been prevented. In one case, a fraudulent wire transfer request for US$1.5 million was processed by SS&C at 1:18 EST on March 16, 2016. The timing precedes a time stamp showing the approval of the last two of the requisite four SS&C employees needed to sign off.

When did SS&C finally wake up to the theft? Seven times was apparently the charm. SS&C contacted Thomas Funk, Tillage Commodities Fund's founder and managing partner after the seventh wire transfer was approved by Martocci and his colleagues. Had the requested US$750,000 been transferred, Tillage's entire account at First Republic Bank would have been wiped out.

Tillage's own conclusion: "Either SS&C processed this series of fraudulent wire transfer requests without any review whatsoever, in total abdication of its obligations – or SS&C knowingly facilitated the fraud," it says in its complaint.

Lisa Solbakken, a partner with Arkin Solbakken, the New York law firm representing Tillage, would not comment on the lawsuit or provide further details on the status of Tillage Commodities Fund. She would only say that her client is no longer trading or accepting any new monies.

What does SS&C have to say?

Based on a statement issued to FinOps Report, SS&C won't be quickly settling out of court because it doesn't think it did anything wrong. In the statement, Anthony Cerroni, global head of investor services for SS&C GlobeOp says the looks forward to responding to Tillage's "unfounded and misleading" allegations in court. SS&C will determine through the litigation process how a security breach at Tillage may have opened the door to the fraud.

Cerroni's statement describes the events as "an unfortunate incident caused by the presentation of valid credentials by unknown third parties who had access to Tillage specific information." SS&C's defense: the credentials presented included authorized signatures of two officers of the Tillage Fund — including that of the fund's founder — in the same form as prior wire transfer requests from the fund."

SS&C has not fired either Martocci or any of the other employees involved with wiring the funds to the Chinese hackers. Cerroni concludes his statement saying "SS&C has, and has always had, robust procedures and controls in place that are regularly reviewed and updated to ensure the protection of client funds."

As for the valid signatures that Cerroni says were received, Tillage's lawsuit says that they were invalid. In attempting to help Tillage retrieve the stolen funds, SS&C did report the theft to the Hong Kong police on March 24. However when it did so, it said it had received emails from known contacts at Tillage with signed letters of authorization provided with valid signatures on SS&C's standard form. "Not one of the subject wire transfers reflect valid signatures," insists Tillage in its complaint. "The signatures used by the fraudster were copies that were, on information and belief, obtained from SS&C's own unsecure system and were submitted on forms not used by Tillage or SS&C at any point during the course of the 4-year relationship."

The lawsuit does not specify how Tillage found out the details of SS&C's report to Hong Kong police, but it would presumably have been handed over by SS&C. However, Tillage alleges that SS&C has refused to provide Tillage with all of its communications with the Chinese fraudsters.

In its statement to FinOps, SS&C never addresses why the badly written emails seeking the transfer of so much money so quickly to the accounts of a Chinese technology firm didn't arose any suspicions. SS&C also never directly addresses any of Tillage's other allegations nor would it respond to FinOps' question about how it plans to address the possible concerns of current and future clients, as well as clients acquired from the purchase of Wells Fargo's global fund services business announced on September 14.

Regardless of how the case pans out, at the very least it should give fund administrators and their clients reason to think hard about their respective cybersecurity practices. Even if non-bank fund administrators may not be subject to regulatory action, they face legal action from their customers. That's not to mention the reputational risk at stake. Asset managers, in turn, also need to consider the liability they may shoulder if their administrators are spoofed with data hacked from the asset managers' own systems.