



## A \$1.5MM Fraud Mystery

### *Who is Responsible for Heist that Closed a Business?*

By Tracy Kitten | August 16, 2013

Between December 2012 and January 2013, Efficient Services Escrow Group of Irvine, Calif., had \$1.5 million drained from its account with First Foundation Bank. Three separate wire transfers were made to accounts in Russia and China, yet no one raised a flag until Feb. 22, when it was too late to recover most of the funds.

On Feb. 28, the California Department of Corporations stepped in and froze the escrow company's activity.

Since then, a state investigation determined Efficient Services was the victim of a cyber-attack. But the escrow company, unable to make up for its losses, has closed.

This incident stands now as one of the largest account takeover cases on record, and it leaves industry experts puzzled about how such fraud losses could go undetected for so long.

"In December 2012, a small amount goes out to Russia. And then, in January, they lose \$1.1 million," says cybersecurity attorney Joseph Burton, managing partner for the San Francisco office of the law firm Duane Morris. "You have to ask yourself, 'What happened?'"

#### **Fraud Timeline**

Neither Efficient Services nor First Foundation responded to requests for comment, but the facts of the case are found in public documents.

According to the California Department of Corporations, the first fraudulent wire, totaling \$432,215, left Efficient Services Escrow's account on Dec. 17. Ultimately, that withdrawal was recovered. But on Jan. 24 and Jan. 30, two more wires, each totaling just more than \$563,000, left the account, and those funds were not recaptured.

The Department of Corporations was notified of the losses by Escrow Agents' Fidelity Corp., the fidelity insurer for the independent escrow industry. Efficient Services Escrow reported to the EAFC on Feb. 22 that its trust accounts reflected shortages totaling more than \$1.5 million, according to public records.

At that point, the Department of Corporations launched an investigation and determined that a "cyber theft" was to blame for the losses.

On Feb. 28, the department froze the company's escrow activity and in March appointed Peter Davidson of California law firm Ervin, Cohen & Jessup LLP to be the company's conservator. Davidson could not be reached for comment about the work being done to

recover the lost funds. But according to the filings recorded with the Department of Corporations, no lawsuits have been filed between the escrow company and its bank.

The Department of Corporations does note that Efficient Services Escrow had previously been cited for lax bookkeeping and record-keeping practices.

The state says the escrow company, at the time the unauthorized wires were sent in January, was not in compliance with state regulations surrounding monthly trust account reconciliation. A regulatory examination conducted in September 2012 also noted that Efficient Services Escrow was not maintaining books and records in accordance with the Escrow Law.

"Respondent [Efficient Services Escrow] had been previously warned during its regulatory examination in 2009 regarding its then failure to maintain proper books and records," state records say.

According to fraud blogger Brian Krebs, who first reported the Efficient Services Escrow incident on Aug. 13, the bank initially thought the losses resulted from embezzlement, not an account hack.

"Efficient's co-owner Daniel J. Crenshaw said the bank produced a report shortly after the heist concluding that the missing funds were stolen not in a cyberheist but instead embezzled by an employee of Efficient Services," Krebs writes. "Crenshaw said the bank later backed away from that claim, after the state appointed a local forensics expert to examine the controller's computer; sure enough, they discovered that the system had been compromised by a remote access Trojan prior to the heist."

### **Who is Responsible?**

The Efficient Services heist goes on record as one of the largest account takeover incidents ever reported, says attorney Burton, a noted expert on these crimes. Only the June 2010 Global Title Services theft, which resulted in \$2 million in fraudulent transfers and just over \$200,000 in unrecovered losses, is larger, he says.

And the case reopens the question that has been hotly debated in the courts over the past few years: Who is responsible for such fraud incidents - the bank or the customer?

Burton and Dan Mitchell, the attorney who represented fraud victim PATCO Construction Inc. in its federal appeal of an account-takeover ruling, offer their analysis of this case and how it might play out.

The first big question is: How did the fraud go undetected?

"It was a foreign transfer, and this company never did foreign transfers," Burton says. "Shouldn't there have been better follow-up from the bank? Here goes \$1 million to China for a client that never has sent money overseas."

Mitchell, an attorney for Maine-based firm Bernstein Shur, shares Burton's curiosity.

"In the news, we're reading all the time about cyber-thieves and hackers in Russia and China," Mitchell says. "Perhaps [the bank] just didn't monitor the transaction, or it might be that the bank's systems were not robust. I don't see how this could go unnoticed."

But clearly something happened on the customer's end, too, to allow credentials to be stolen and for the account to be breached.

"This is, again, a case in which it looks like there was a piece of malware on the client's computer," Burton says. "And that is going to touch on the same issue we saw in the Choice Escrow and PATCO cases, which is: Where does the client have some potential responsibility?"

In June, Missouri-based Choice Escrow Land Title LLC appealed a district court's ruling in a legal dispute with its former bank over an account takeover incident dating back to 2010 to an overseas account in Cyprus. Choice Escrow is awaiting a ruling in that appeal.

From Mitchell's perspective, both parties appear to bear some blame for this incident.

"The first transaction should have looked suspicious," he says. "And on the customer's end, not reporting the loss for such a length of time seems strange. The escrow company presumably should have been super-vigilant. There are things they could have done, and you would think, as an escrow company, they would have been accustomed to watching transactions in their account very closely."

The Efficient Services is unique, says Mitchell, because the State of California now has a role in the investigation. "I've never seen that before in an account takeover incident," he says.

Escrow companies are responsible for safeguarding funds, Mitchell notes. "So if escrowed funds are at risk, then the state may have the right to step in right then and there to protect those escrowed funds," he says. "My assumption is that [Efficient Services] lost the money and could not replace it, so the state exercised its regulatory prerogative and stepped in."

And while no litigation has been filed yet, Burton says a civil suit is a likely route to answer the open questions and resolve the issue of responsibility.

"I don't think this escrow company has much choice but to sue the bank," Burton says. "They've been put out of business."

*Dan Mitchell is a shareholder and member of Bernstein Shur's Business Law Practice Group and Data Security Team. He can be reached at 207 228-7202 or [dmitchell@bernsteinshur.com](mailto:dmitchell@bernsteinshur.com).*