

Wealth Managers: Lessons from the HSBC Data Theft

A New Business Model for Private Bank Employees?

Dec. 17, 2009

We don't know how many client files "Hervé" and his mysterious female companion have stolen from their employer [HSBC](#). The estimates range from "under 10" (HSBC statement) to 130,000 (statement of the French prosecutors). But fact is that sensitive data of a Private Bank have again been stolen by an employee of that bank. This employee and his accomplice have apparently tried to sell the data to Mobsters and after failing to do so, the files have fallen into the hands of government authorities. The French government may or may not use them to prosecute tax evading citizens based on this evidence. The French authorities also may or may not forward some of the files to other governments.

This is not the first case of employees of a Private Bank to steal data from their employer and make money of the stolen goods by selling them to third parties who can use them to prosecute or blackmail the bank clients. The recent case of Liechtenstein's [LGT](#) is only one other example. We suspect that many cases have never been disclosed because the banks either quietly paid their former employees to return the data or the buyer of such data – be it governments or criminal organization - did not give any notice to the public.

It seems that disaffected employees of Private Banks have discovered a new business model. You can call this new business "Taking advantage of legal arbitrage". In short: What they do is illegal say in Switzerland, Luxembourg or Liechtenstein. But it is legal and is encouraged in Germany, France, the USA and many other countries. This creates the opportunity to illegally steal files in one country, cross a border and sell the data perfectly legal to the tax inspectors of this country. Such data are an asset that is worthless to the thief in one country but perfectly valuable in the neighboring market.

What can banks do to prevent their employees from taking part in such a new business model? For one, they can increase the transaction costs, namely strengthen the protection of their data systems. Unfortunately this seems a futile effort as every relationship managers knows the names and addresses of his book of clients. It is also extremely difficult to control internal staff who handles the information system – many of them being shrewd soft- and hardware experts.

A second option is to increase the severity of the punishment for such breach of confidentiality. This is probably an even more fruitless effort as the neighboring countries are not willing to execute such punishment when an ex-employee of a bank seeks refuge from prosecution.

A third option is to reinforce the moral and ethical standards among bank employees and thus prevent them from engaging in the file-theft-business. However, as the ethical behavior of many banks is being questioned around the globe, employees can in turn easily justify their unlawful actions to themselves.

A fourth option would be to make the stolen assets worthless. If there are no more potential buyers for confidential customer files the business is gone. But this would be only possible when the banks convert offshore to onshore customers. Or, alternatively, show the door to all customers who are unwilling to co-operate.

Given the weakness of options one to three only the latter alternative is realistic. Whistle blowing, breach of confidentiality, and the outright theft of files recently has been enormously popular among some employees of offshore banks. It is almost impossible to stop such individuals. They have the potential to completely destroy the reputation of financial centers like Liechtenstein, Luxembourg or Switzerland, and a lot of damage has been done already. It is about time to eliminate the root cause for such behavior.