

Data theft and the purchase of stolen data

*Dr Alexander Ressos, TEP
Attorney-at-Law (Switzerland), Solicitor (Hong Kong),
Solicitor (England & Wales)*

The collapse of banking secrecy was accelerated by the theft of client data. In 2008, the German tax authorities purchased from a former employee of the Liechtenstein bank LGT a set of data on German clients, which led to the investigation of hundreds of German taxpayers, among them the chief executive of Deutsche Post, Klaus Zumwinkel, who was convicted of tax evasion.¹ In the following years, several German states, among them North Rhine-Westphalia, purchased data carriers with client data stolen from Swiss banks, paying millions of euros to the informants. The data led to investigations of thousands of German taxpayers and to a wave of voluntary disclosures.²

The most famous data theft concerned the Geneva branch of HSBC. Hervé Falciani, an IT employee of HSBC Private Bank in Geneva, copied the data of more than a hundred thousand clients and handed them to the French authorities in 2008 and 2009. The French government shared the data with other governments, so that the so-called Lagarde list led to investigations in many countries. Falciani was convicted in absentia by the Swiss Federal Criminal Court in 2015 for aggravated economic espionage.³

The purchase of stolen data raised legal questions in both countries. In Switzerland, the theft and disclosure of bank data was a violation of banking secrecy under Article 47 of the Banking Act and, when committed for the benefit of a foreign state, a crime of economic espionage under Article 273 of the Criminal Code. The Swiss authorities prosecuted several informants and also investigated German tax officials who had participated in the purchase of data. In Germany, the use of stolen data as evidence in criminal proceedings was challenged, but the German Federal Constitutional Court held in 2010 that it could be used to justify a search warrant.⁴

The data thefts showed that banking secrecy could be undermined from inside the banks. An employee with access to client data could copy it and

sell it to a foreign government, whose use of the data the criminal law of Switzerland could not prevent. The risk of disclosure through data theft made banking secrecy unreliable for clients and contributed to the wave of voluntary disclosures and regularisations that followed.

1 Notes

1. On the purchase by the German Federal Intelligence Service and tax authorities of data from LGT (Liechtenstein) in 2008 and the conviction of Klaus Zumwinkel for tax evasion in 2009, see the press reports and court records. To be verified. ↩
2. On the purchase of data carriers with client data of Swiss banks by German states (in particular North Rhine-Westphalia, from 2010) and the resulting investigations and voluntary disclosures, see the press reports and the publications of the German tax authorities. To be verified. ↩
3. On the theft of HSBC Private Bank (Suisse) client data by Hervé Falciani, its transmission to the French authorities (2008/2009), the "Lagarde list" and Falciani's conviction in absentia by the Federal Criminal Court on 27 November 2015, see the published judgment and press reports. To be verified. ↩
4. On Article 273 of the Swiss Criminal Code (economic intelligence service) and its application to the sale of bank data to foreign authorities, and the decision of the German Federal Constitutional Court of 9 November 2010 (2 BvR 2101/09) on the use of purchased data for search warrants, see the published decisions. To be verified. ↩

For general information only. This article does not constitute legal or tax advice, does not replace advice on an individual case and creates no lawyer-client relationship. It reflects the legal position as of September 2026.

Online version: helveticaregister.com/basel-data-theft-and-the-purchase-of-stolen-data