



## **SWIFT Statement**

**Francis Vanbever**

**Chief Financial Officer, Member of the Executive Committee, SWIFT**

European Parliament Hearing

04 October 2006

### **Introduction**

Thank you

Madam President, Mr Chairman. Thank you for giving me the opportunity to present the facts related to the submission of limited data sets by SWIFT to the US Treasury and to provide input to your analysis of this complex issue.

SWIFT takes its data protection responsibilities very seriously. SWIFT is a private company created in 1973 for the exchange financial messages. Integrity and the confidentiality of its customers' data has always been its highest priority. Protecting the confidentiality of SWIFT's users' data lies at the core of our business.

It is very important that you understand that SWIFT adopted in 1993 a policy for compliance with requests from judicial authorities. SWIFT is not insulated from lawful subpoenas and judicial warrants. This compliance policy was communicated in 1993 by the SWIFT Board to all its members. The policy was then incorporated in our User Hand Book, which is the official contract between SWIFT and all our users. Contrary to what has been written, our data disclosure policy has been known to all our users for over 10 years.

In October 2001, our US Branch received subpoenas from the US Treasury Department in relation with the tracking of terrorism financing. We invoked our compliance policy, which includes in-depth legal reviews in the US and Europe. These reviews concluded that we had to comply with the subpoenas, and that, in doing so, we would not breach European laws. In addition, SWIFT did its utmost to protect the data of its customers. Private companies such as SWIFT must respect both the spirit and the letter of the law, which we do. Therefore, we strongly object to the opinion expressed in last week's Belgian Data Privacy Commission advisory report that SWIFT has not fully respected the Belgian and European data protection laws. But we strongly endorse one of the conclusions of the report: the call for renewed cooperation between the European Union and the United States. We believe that the issue of balance between the need to fight terrorism and the right to privacy can only be resolved by political leadership. Governments must define the boundary between security and data privacy, and we welcome initiatives to that effect.

\* \* \* \* \*



With respect to the specifics of the SWIFT case, let me start by providing you with the context of what SWIFT is and the role it plays in the international financial system. I will then move on to describe how we responded to the compulsory subpoenas that we faced in the US.

## **About SWIFT**

I will be relatively short in presenting SWIFT's activities, as you can refer to the background material sent yesterday for further details.

### **1. SWIFT is solely a messaging intermediary**

SWIFT is an industry-owned cooperative. It was created in 1973 by a group of banks that wanted to replace the telex with a secure and reliable means of transmitting financial instructions between institutions.

Today, our company provides secure, standardised messaging services and interface software to over 7,800 financial institutions in 206 countries worldwide.

SWIFT's sole function is to act as a global messaging intermediary between financial institutions. We are not a bank. Private individuals do not have access to SWIFT. We do not hold accounts or assets of any customers. We are not a clearing or settlement system.

SWIFT can be viewed as the 'plumbing' between financial institutions.

### **2. SWIFT customers own and control their message contents**

SWIFT acts as a processor for its users. We offer a pure messaging service. We transmit messages on instructions from our users. We do not have any contact with the customers of our users.

### **3. SWIFT messaging services must be secure, reliable & resilient**

SWIFT has been defined as a critical infrastructure by governments and central banks.

Our focus is on maintaining the availability, confidentiality and integrity of our message data and related systems. For this, we invest heavily in security.

To recover from the potential loss of facilities, we operate multiple operating centres on different continents, with full data mirroring. For operational purposes, all messages are stored in all operating centres for a period of 124 days. This includes our operating centre in the US.

### **4. SWIFT is overseen**

As SWIFT is neither a bank, nor a settlement system, it is not subject to financial regulation. However, given the large and growing number of payment systems which have become dependent upon SWIFT, it has acquired a systemic character.

For this reason, the central banks of the G-10 have set up a system of cooperative oversight. The National Bank of Belgium (NBB) is the lead overseer as SWIFT is incorporated in Belgium.



The oversight objective is to ensure that SWIFT has the appropriate governance arrangements, structures, processes, risk management procedures and controls that enable it to effectively manage the risk that it may otherwise pose to financial stability.

SWIFT's relationship with the National Bank of Belgium and its overseers is based on trust, transparency, and absolute confidentiality.

\* \* \* \* \*

## **SWIFT compliance with UST subpoenas**

Let me now turn to SWIFT's compliance with the subpoenas issued by the US Treasury

### **1. SWIFT only complied when subpoenas confirmed as compulsory**

Following the September 11, 2001 attacks, SWIFT received subpoenas from the Office of Foreign Assets Control of the US Treasury Department. A subpoena is a compulsory order to provide information.

The subpoenas were served in the US to SWIFT's US branch for information stored in the US operating centre.

Upon receipt of the subpoenas, SWIFT activated its 'compliance policy', adopted by the Board of Directors in the early 1990s. As I have already mentioned, this policy is included in our customers' contracts and public on our website. It states clearly that, while SWIFT takes all necessary measures to ensure the highest degree of integrity and confidentiality for the data that we transport, we have to comply with legal subpoenas and warrants issued by authorities. In such cases, data might be transmitted to authorities. This policy is well understood by our customers, since, as financial institutions, they face similar obligations.

In line with this published policy, SWIFT verified the legality and the compulsory nature of the subpoenas with its external legal counsels.

They confirmed that the US Treasury had jurisdiction over SWIFT, and that SWIFT was subject to the subpoenas because of its substantial operations in the US, including data storage.

SWIFT concluded that the subpoenas directed to the US branch were issued under the authority of the US President and the US Congress and were lawful and compulsory under US law. SWIFT recognised that US law provided for civil and criminal penalties, including fines and imprisonment for failure to comply with the subpoenas.

SWIFT concluded that, as a processor of data on behalf of its customers and given its disclosed compliance policy, SWIFT's compliance with the US subpoenas would not lead to a breach in its obligations under European data protection law.

On this basis, the SWIFT Board of Directors concluded that it had no choice but to comply with these subpoenas.



## **2. SWIFT obtained unique protections & assurances**

We have a responsibility to protect our customers' data to the largest extent possible, so we managed to obtain unique and extraordinary protections and assurances. From the very beginning, SWIFT established the key principles of a) purpose limited to terrorism investigations only and b) protection of the limited sets of data that were delivered. These protections and assurances were documented in a Memorandum of Understanding with the US Treasury.

## **3. Data subpoenaed by the US Treasury is limited**

SWIFT narrowed the scope of the subpoena to a limited set of data.

Contrary to media reports, the subpoenas are narrow and by no means cover all data stored in SWIFT's US operating centre.

## **4. Searches targeted exclusively to ongoing terrorist investigations**

SWIFT narrowed the scope further by restricting the UST's access and use of the subpoenaed data. The data can only be searched for the unique purpose of ongoing terrorism investigations.

The US Treasury is not authorised to browse through the data provided by SWIFT; they cannot go 'fishing'. This is not a data mining process.

The US Treasury is only able to see information which is responsive to targeted searches based on ongoing terrorism investigation.

The US Treasury cannot search the data for evidence of non-terrorism related crime. SWIFT has explicitly excluded searches for tax evasion, economic espionage, money laundering or any other criminal activity. As a result, the US Treasury may only view a very tiny fraction of the data provided. A record is made of every query made.

## **5. Subpoenaed data is protected**

SWIFT obtained safeguards to ensure that the US Treasury stored the subpoenaed data in a secure environment and treated it confidentially.

## **6. These protections are audited by SWIFT and external auditors**

Concerns have been raised that all systems can be abused. In this case, we "trust but verify". SWIFT knows a lot about risk mitigation—that is our business. So, SWIFT has instituted controls to ensure, to the fullest extent possible, that the US Treasury respects these limitations and protections, and that searches of the data are targeted exclusively on existing terrorist investigations. Based on these controls we believe the chance of abuse are as close to zero percent as possible.

SWIFT has representatives on site at the Treasury. They review every query. They can stop any query in real time if they are not satisfied that it is related to an ongoing investigation into terrorism financing.



SWIFT has commissioned an external independent security and technology consulting firm to provide assurance that the protections and conditions are fully adhered to, all under best practice audit standards. They review the search records and give SWIFT the assurance that the data has only been viewed and used for terrorism investigations. The auditors also review the end-to-end security of the system and provide SWIFT with the assurance that the data has been protected from unauthorised access.

SWIFT's Board of Directors received reports from the independent auditors twice a year.

Via these mechanisms, SWIFT has maintained virtual control over the subpoenaed data.

## **7. SWIFT's compliance is overseen**

Compliance with the US Treasury subpoenas is supervised by SWIFT's Board of Directors. In addition, SWIFT has kept its G10 central bank overseers informed about the US subpoenas and the protections.

\* \* \* \* \*

## **Closing**

In summary, SWIFT's compliance with the US Treasury subpoenas has been legal, limited, targeted, protected, audited and overseen. It has also been compulsory.

SWIFT obtained from the US Treasury protections and controls that met both its requirement to follow the law and its obligations to protect the confidentiality of its members' data. SWIFT believes it all it could to get the balance right.

The question today is how society can balance the right to personal privacy with the duty to protect personal security. We strongly subscribe to calls for a renewed political dialogue between Europe and the United States on this issue.

Private companies can play their part through upholding the law, but they cannot make policy.

Ultimately we are dependent on our governments and elected officials to frame the law.

Thank you for your attention

\* \* \* \* \*