

COMMUNICATION FROM SWITZERLAND

E-banking in Switzerland

Addendum

The attached communication has been received from the delegation of Switzerland with the request that it be circulated to Members of the Committee on Trade in Financial Services.

ANSWERS TO SUPPLEMENTARY QUESTIONS

At the meeting held on 16 May 2003, Members of the Committee on Trade in Financial Services raised a number of questions on the communication entitled *e-banking in Switzerland* (S/FIN/W/26). The following answers are an attempt to follow-up on the discussion. This document is for information purposes only.

Q.1. The concept of technological neutrality was questioned by several Members.

1. In Switzerland's view, technological neutrality is an essential assumption of the GATS. It means that services are subject to the same commitment regardless of the technology used to provide them. Violation of this principle could damage commitments already undertaken in previous negotiations. Technological neutrality does not preclude regulations from applying to a specific means of delivery of a service, as long as it fits into the corresponding commitment.

Q.2. What is the impact of e-banking on the financial sector? Are there any surveys on the implications, including in developing countries?

2. It is difficult to assess the impact of e-banking on the financial system in developing and developed countries because the evolution is relatively new. The lack of reliable data is an additional problem.

3. Some studies have been conducted within the World Bank or UNCTAD on the opportunities of e-finance for emerging markets. One conclusion that needs to be assessed is that some countries may have unsophisticated financial systems today with limited services and poor infrastructure. To the extent that financial services are provided, they might reach only select groups: urban customers with high net worth, state enterprises, and large agribusiness rather than small and medium-size firms, farmers or micro-enterprises. Resource allocation and intermediation costs could be improved through e-finance.

Q.3. Can sound and safe banking be achieved through electronic means? Is the supervisory authority aware of problems affecting Swiss consumers?

4. E-banking is an extension of traditional banking and does not *per se* bring additional concerns. The use of e-banking can exacerbate existing supervisory concerns. At the time being, there is no specific regulation in Switzerland with respect to e-banking, including when performed on a cross-border basis.

5. As far as prudential regulation is concerned, the Swiss banking surveillance authority distinguishes between consumer protection and the avoidance of systemic failure. The banking surveillance authority in Switzerland supervises banking institutions in Switzerland and thus guarantees customers of sound practices by supervised institutions. According to Swiss banking legislation foreign banks offering banking services from abroad either by means of the Internet or by other means are not subject to Swiss banking supervision. Swiss law thus prohibits banks from misleading consumers with regard to their origin. The law wants it to be clear for the customer as to whether a bank is authorised, hence supervised, in Switzerland. It is then up to the customer to assess the strength of the institution he is willing to deal with. No problems have been reported to the banking surveillance authority concerning misled customers.

6. As for avoiding systemic failure, the banking surveillance authority applies the general principles elaborated under the auspices of the Basel Committee on Banking Supervision and its dedicated working group on electronic banking. For a summary of the results of this group, please refer to Part I of our communication S/FIN/W/26, dated 30 April 2003. The banking surveillance authority has not encountered any difficulty with cross-border banking. When concerns arise, it seeks cooperation from the home country of the institution to avoid any gap in supervision. This approach does not preclude any future specific regulation for e-banking. Such regulation would be taken for prudential reasons only and not discriminate between foreign and domestic suppliers.

7. The banking surveillance authority does not know of any Swiss bank having been contacted by foreign surveillance authorities in relation with the operation of their websites.

8. Operational risk is not specific to e-banking either. All financial institutions rely heavily on their IT infrastructure. Brick-and-mortar financial institutions make intensive use of electronic means. A break-down of its IT system would be very damaging to any financial institution. The terrorist attack on 11 September 2001 demonstrated the strength of IT systems management by the banks. Moreover, operational risks (including IT systems) form part of the overall assessment conducted by external auditors reporting to the banking surveillance authority. In addition, focussed tests are being carried out to assess protection against attacks such as “hacking”, “sniffing”, “spoofing” or “denial of service”.

9. In a recent survey conducted by the banking surveillance authority, banks reported no problems relating to the operation of their websites, apart from short-term system interruptions.

Q.4. Where is the contract between the consumer and the service provider enforceable?

10. Unless otherwise agreed between the parties, enforceability of international contract law is ruled in the Federal Act on Private International Law¹. This act is technologically neutral and it is not foreseen to modify it because of technological developments. Hence, general rules applicable to international transactions will continue to apply.

¹ This Act is to be found on in German at <http://www.admin.ch/ch/d/sr/c291.html> , in French at <http://www.admin.ch/ch/f/rs/c291.html>, in Italian at <http://www.admin.ch/ch/i/rs/c291.html> and in English at <http://www.umbricht.ch/de/news.html>. The latter version is unofficial.

Q.5. Why did the virtual-only bank close down?

11. During the so-called Internet bubble many companies were created and later shut down. It seems that the virtual-only bank was one of those. It has to be stressed that many brick-and-mortar banks set up projects for electronic banking. Some of them have developed and are performing quite well, while others have been resized or abandoned. It is also worth noting the difficulty for a bank to work on a virtual-only basis. In spite of the liberal regime, customers in Switzerland occasionally request physical contacts with their banks for more sophisticated services. It is interesting to note that in Hong Kong, the Internet bank uses the retail network of a sister bank within the same banking group.

12. It is worth noting that a virtual-only institution is still operating in Switzerland with a banking license. It is mainly active as a broker and offers portfolio management services. It can be reached at www.swissquote.ch.

Q.6. How do money laundering rules apply to e-banking transactions?

13. The Swiss banking surveillance authority is convinced that the use of e-banking does not fundamentally affect the relation between the banker and his customer.

14. As far as transactions are concerned, risks are similar if the transaction is proceeded through the Internet or through more traditional means. The banking surveillance authority is convinced that the current provisions for the monitoring of relationships and transactions are adequate for electronic banking.

15. Entering in a business relation by electronic means is considered as another non face-to-face relation. The Swiss anti-money-laundering framework for banks is twofold in this regard. While the *Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence* of 2 December 2002 ("CDB 03") sets the rules for the verification of the contracting partner's identity and the identification of the beneficial owner, the *Anti Money Laundering Ordinance* ("AML-Ordinance") by the Swiss Federal Banking Commission contains special due diligence rules for business relations and transactions involving higher risks.

16. For e-banking, there are no specific rules regarding identification and monitoring procedures. The general rules apply also to e-banking. The CDB 03² states that "*in case of business relations entered into by correspondence or by Internet, the bank verifies the identity of the contracting partner by obtaining a certified copy of an official identification document, as well as the confirmation of the domicile indicated*". Hence, it is not possible, for the time being, to open an account by electronic means only. In order to establish the identity of the beneficial owner, usual procedures are equally applicable.

17. In addition, the AML Ordinance qualifies all non face-to-face business relations as associated with higher risks requiring banks to carry out additional examinations. The absence of a meeting with the contracting party and the beneficial owner is one of the criteria³ to qualify a business relationship as more risky. If the bank identifies a business relationship as more risky, it shall then further clarify the identity of the contracting party and of the beneficial owner. Clarification means include:

² This document is, with respect to verification of the identity of the contracting partner and the identification of the beneficial owner, binding for all financial intermediaries, according to the *Ordinance of the banking surveillance authority on money laundering* (Art. 14).

³ Other criteria include: the location or the domicile of the contracting party and the beneficial owner or their nationality, the nature and the place where the business activity of the contracting party and the beneficial owner happens, the type of services or products requested, the origin or destination of frequent payments.

additional information from the contracting party and the beneficial owner, inspection of business operations from the contracting party and the beneficial owner, and consultation of publicly available databases.

18. The *Ordinance* also requires financial intermediaries to set up IT systems to trace any suspicious transactions. The idea is to filter transactions which are more risky, according to certain standards. E-banking does not affect this process.

19. No difficulties have been reported to the banking surveillance authority regarding the implementation of money laundering rules in the context of e-banking. Banks and other financial intermediaries are in the process of implementing these rules. They have not found difficult issues in this regard, apart from very technical difficulties, which are being tackled.
