

**Murat Volkan Dülger**

## **Electronic Banking And Security**

Electronic banking in Turkey is becoming widespread in number due to lower operating costs associated with it.

As it was in the form of automatic teller machines and telephone transactions formerly, the banking sector is now providing internet usage to build up a new delivery channel for banking services so as to provide much lower costs. In this matter, there have been great investments and practices recently. As well as for customer orientated transactions, the information technology is also being used for interbank affairs such as electronic check clearing system and direct debit system. Thus, it has also provided a change in banking sector structure due to the fact that no traditional bank would stand without an internet strategy.

Now Turkish Banks are aware of the fact above and offering a wider range of services, in another name "online banking" from their internet branches. As banks have their own websites, customers are able to manage their transactional applications via such websites including credit card transactions, money transferring from account to account, application for a loan, opening up a new account etc. In practice, banks make a contract with the customers within the framework of the general banking provisions and set a password for customer to access to the system. With options just a click away, customers most widely-use credit cards with online transactions which improve efficiency and effectiveness of online banking. At this point it is necessary to take a look at the security measures on the ground to eradicate fraud in electronic banking.

To provide security on internet banking, some programs called SSL (Secure Socket Layer) and SET (Secure Electronic Transactions) have been developed. As these programs being used by most banks in Turkey, it is provided that any party in the electronic trading cannot see the password of the credit card of another. This is because; the programs encode every data between customer (card bearer), trading firm and the bank. Therefore, it would prevent anyone from decoding the passwords or any other data. Another security system is called the usage of so-called "virtual card". Normally, a virtual card does not have any limit and by using such card, the customer only authorizes the bank to withdraw money from the actual account of the customer.

While banks are benefiting from technology to better protect their systems and to prevent any illegal interference, the current legislation in force, also imposes them some responsibilities and liabilities. Firstly, the banks are liable to inform their customers of the new technological systems applied by the bank and the risk factors. The bank should also assist the customers in protecting their account safety. In this respect, for instance, in each entrance to the bank's website, the banks declare the last card usage with the date and other details in advance of next transaction with card. Besides, customers should be informed of their expenses exceeding their limits or of the orders given from exceptional IP addresses than a usual one. The other liability of the banks is to take measures concerning system operation and prevention of data errors. If any error occurs, damage to be incurred, would be on the bank.

By the reason of problems arising from credit card usage, Code of Banking and Credit Cards numbered 5464 was enacted on 23<sup>rd</sup> February 2006. With the 8<sup>th</sup> clause therein, card issuers are obliged to institute a system which provides secure utilization of cards and takes relevant measures for the effective filing of notifications, complaints and claims. In addition to this provision, article 15 provides that at the end of each use of a credit card, the card holder should be provided with a receipt proving the purchase and the banks are required to draw up a confirmation deed before effecting a payment to trading firm.

Another problematic issue of internet banking is customers' money in bank deposit accounts being transferred to another account by third parties who decode the passwords. These fraudulent activities, mostly performed by spy programs spreader on the internet. Banks, usually, are confronted with such customers whose accounts are emptied by an illegal interference. Banks, in such a situation, tend to protect themselves by alleging that they have no liability related to these illegal transactions due to non-liability clauses imposed in contracts against the customer. But in recent decisions of the Court of

Appeal, it is ruled that banks also have liability to provide sufficient protection for the customer against such illegal interventions of third parties via internet.

So in addition to the legislation in force regarding banking transaction, the interpretation of such legislation or any possible gaps in the legislation by the courts usually be in favor of customer in order to provide sufficient protection to the customer who is considered as more vulnerable than a bank. However, this, of course, would not mean that the card holders would have no liability regarding their electronic banking activities. Indeed, a deposit account owner is responsible of duly protection of his/her security as well.

In a recent case before the Court of Appeal the plaintiff's online account was tried to be decoded many times by an outsider and the money in the account was transferred by sixteen different transactions. The defendant (bank) imputed negligence on the plaintiff that he was not using virtual keyboard and not providing his personal computer secured. The Court of Appeal held that there was a negligence of the plaintiff by not obeying the security measures applied by the bank. According to the decision, banks are liable for the slight negligence arising from not complying with duty of objective care as they are considered to be institutions of trust. Basis of this valuation relies on the "theory of trust" which is regulated under article 2 of the Turkish Civil Code. However, it is unfair to hold banks solely liable for illegal intervention to the computer system of the customer as it is not within the area of control of the banks. (Court of Appeal, M.2006/7341, D.22/06/2006). There exists other decisions that indicate the liability of customers who do not provide the sufficient care for the security tools such as passwords which are specifically given for the internet banking. In one of these cases, the Court of Appeal held that the bank has no liability for the damages occurred on customer's side due to the illegal decoding of the password as it occurred due to the fact that the customer was not sufficiently protecting his computer system. (Court of Appeal, M.2003/7705,D.12/09/2003).

In fact, despite of the above stated decisions, it is not always so easy to determine on which side of the dispute there exists a security gap. The lack of sufficient number of precedents is another problem for the practitioners to interpret the matters before them. However, by reading the interpretations of the Court of Appeal between the lines of their decisions, we may say that in case of an illegal intervention to a bank account, determination of evidence, as an initial step, would have a vital importance for the protection of the rights of the customer in order to prove that the customer has already taken every necessary measure to protect his computer system as the Court of Appeal considers that the computers of those customers claiming compensation must have an anti-virus program set up as a protection for the outside attacks.