Ozan Karaduman Managing Associate
ozan.karaduman@gun.av.tr
Gün + Partners, Istanbul

Image: Michal Stefl ovic / Shutterstock.com.

The recent cyber attacks against banks in Turkey: the legal situation

On 8 December 2016, a cyber attack was made against Akbank, one of Turkey's largest banks, and supposedly two other Turkish banks. Akbank released a statement confirming the attack to their IT systems, that it related to the SWIFT system, and stating that they had responded to the attack immediately and taken the necessary precautions. The bank also set forth that the maximum amount of risk faced by the bank is USD $4 million which is covered by its insurance policy. The names of the two other banks which are said to have been attacked are not known and no statement has been released by any other Turkish bank on the issue. In this article, Ozan Karaduman, Managing Associate at Gün + Partners, explains the means of attack against Akbank and the possible legal consequences.

The attack

The statement released by Akbank said very little about the causes of the attack and how it happened. After the attack, a few sources reviewed the situation and wrote about the causes and *modus operandi* of the attack. According to those sources, the attack was similar to the one made against the Central Bank of Bangladesh in which the attackers gained access to the bank's payment credentials in the SWIFT System and succeeded in transferring $81 million. According to an article written by Alper Basaran[1], 'the initial attack vector was spear phishing; the attackers targeted an employee with a Microsoft Office Document containing a malicious macro that downloads the Odinaff malware, attackers then gained persistence and started activities in the bank's network using Windows components. The use of 'legitimate' software allowed attackers and malware to remain under the radar of antivirus software which usually looks for unknown or new files. Attackers collected credit card information and executed money transfer via the SWIFT system. Also seen in previous Odinaff attacks the malware was able to hide logs and SWIFT messages related to the fraudulent transactions made by the attackers.' In her article[2], Fusun Sarp Nebil states that the attackers rearranged the SWIFT message details in order for the payment to be made to an address determined by the attackers instead of the original address. Nebil also commented that it is not clear whether the credit card information had actually been collected. Akbank however has not confirmed any of these details.

Legal consequences

Liabilities of the banks

The main legislation governing the banking sector in Turkey is the Banking Law numbered 5411 and dated 19 November 2005 ('the Banking Law'). The Banking Law does not have a specific and explicit provision regarding the liabilities of a bank in the case of unauthorised access to its IT systems. The Banking Law sets forth that the banks should comply with the applicable legislation and instructions of the Banking Regulation and Supervision Agency ('BRSA') and perform proper internal audit, control and risk management mechanisms.

The piece of legislation that relates more to unauthorised access to banks' IT systems is the Regulation on the Independent Audits on Banking Information Systems and Banking Processes to be Performed by Independent Auditors ('the Regulation') issued by the BRSA. The Regulation sets forth that the banks should comply with the Control Objectives for Information and Related Technologies ('COBIT') standards issued by ISACA. The COBIT standards include good practice provisions regarding information security, the Regulation also states that the security of information is an important aspect that an auditor should examine during the audit of a bank. Article 67 of the Banking Law sets forth that the banks should comply with the Banking Law, the related legislation and the decisions made by the Board of the BRSA. As the Regulation is secondary legislation of the Banking Law and as it states that the banks should follow the COBIT standards, we can conclude that as per Article 67 of the Banking Law, the banks should comply with those standards. As a result, if Akbank and the two other banks that were attacked complied with the COBIT standards, they will not be held liable for an administrative or penal sanction. However, if they have not complied with those standards, the Banking Law sets forth that the BRSA will request that the banks comply with the standards. If the banks still do not comply with them, the directors responsible for compliance will be subject to imprisonment between two to four years and a monetary fine of between TRY 20,000 - 500,000 (approximately €5,000 - €125,000).

If credit card information has also been copied as a result of these attacks, the breach will fall under the scope of the Debit Cards and Credit Cards Law numbered 5464 and dated 23 February 2006 ('the Credit Card Law'). Article 39 of the Credit Card Law states that the responsible directors in the banks that have caused the leakage of the credit card numbers or any other important information due to inattention, imprudence, inadequacy or non-compliance with the rules, will be subject to a monetary fine of between TRY 20,000 - 100,000 (approximately

Image: Celal Erdogdu / iStock / Getty Images Plus / Getty Images

If Akbank and the two other banks that were attacked complied with the COBIT standards, they will not be held liable for an administrative or penal sanction.

€5,000 - €25,000). The terms such as imprudence and inadequacy are broad and vague in nature. However, we believe that if a bank has complied with the COBIT standards, its directors should not be held liable under Article 38 of the Credit Card Law.

There is another important piece of legislation in relation to the breach of IT systems: the Law on Protection of Personal Data numbered 6698 which came into force on 7 April 2016 ('the Data Protection Law'). If credit card data has been exposed as a result of these cyber attacks, the breach will also fall under the scope of the Data Protection Law because the credit card information would most likely be related to an identifiable person, which would make the information personal data. Article 12 of the Data Protection Law sets forth that data controllers (in this case the banks) should take all the necessary technical and administrative precautions to ensure the security of the personal data. Failing to comply with such a requirement would result in an administrative fine of between TRY 15,000 - 1,000,000 (approximately €3,750 - €250,000).

There is currently no secondary legislation related to the Data Protection Law on the proper security measures to be implemented. In the absence of any such specific requirements, we believe that the COBIT standards should be regarded as adequate security measures and the banks should not be held liable under the Data Protection Law because of the breach.

Under the Banking Law, the Credit Card Law and the Data Protection Law, the sanctions provided do not penalise the organisation for the security breach but for not taking the necessary precautions. This is reasonable because technology evolves every day and with each security development, someone somewhere will be working on breaching that newly created security wall. It has become a race between the securers and the hackers. The only thing one can expect from the banks is that they take the utmost efforts to secure the information of their clients. If the lawmaker were to sanction the banks for every breach, this would put a burden on the banks in an area that they cannot predict or control. Moreover, this would create another motive for the hackers as they would not only be receiving funds illegally but they would also be punishing the banks from a legal perspective.

Liabilities of the hackers

The liabilities of hackers who breach the IT system of a bank are determined under Article 244 of the Turkish Penal Code numbered 5237 and dated 26 September 2004 ('TPC'). Article 244 of the TPC sets forth that if a hacker breaches the IT system of a bank and then damages, destroys, changes or makes the data inaccessible or puts data into the system or transfers the data; that hacker will be subject to imprisonment from between nine months and four and a half years. If the hacker financially benefits from that breach, he/she will be subject to imprisonment from between two to six years and also to a monetary fine of between TRY 100,000 - 500,000 (approximately €25,000 - €125,000).

In the attacks discussed in this article, the hackers breached the IT system of the banks, transferred the data to another system and benefited financially. As the crime was committed within Turkey (the servers of the banks are located in Turkey), the attacks will fall under the scope of Article 244 of the TPC and the hackers (if caught) will be subject to imprisonment of up to six years and also to a monetary fine up to €125,000. They will also be liable for compensating the banks for the losses incurred.

1. http://securityaffairs.co/wordpress/54495/malware/odinaff-attack.html
2. http://t24.com.tr/yazarlar/fusun-sarp-nebil/swift-saldirisi-3-turk-bankasinda-yasanmis-bddk-bankalari-uyardi,16136