Unchanged password: the liability of a maintenance services provider

Commercial Court of Nanterre, 3rd Chamber, n°2013F00738, 5 February 2015

The Commercial Court of Nanterre held a maintenance services provider liable for failing to warn its client about the risks incurred for not changing its PABX telecommunications system password.

Fast Lease is a car rental company specialised in short term rentals mainly to small and medium sized businesses. To facilitate communications with its clients, Fast Lease rented a PABX system (an internal private telecommunications network with a gateway to the public network) from Normaction SA and entered into a maintenance services agreement with its sister company, AET Normaction.

Both Normaction SA and AET Normaction faced insolvency issues and were bought by Nérim and United Télécom et Travaux ('UTT'). When Nérim bought Normaction SA, it inherited the PABX lease agreement with Fast Lease as well as the telephone subscription agreement and when UTT bought AET Normaction it inherited the maintenance services agreement with Fast Lease. Thus, the Commercial Court ruling concerns Fast Lease and its new contractors, Nérim and UTT.

The PABX system agreement included the installation and rental of the PABX equipment as well as subscription to telephone services. The maintenance services agreement provided for a yearly visit to check on the condition of the equipment and system by AET Normaction as well as a general duty to advise and inform Fast Lease.

Access to the PABX system required the use of a password which is, by default, '0000' when installed for the first time. To fully secure access to the system, the user must change the default password, which must remain confidential.

Fast Lease had not changed its PABX password for about three years, before Normaction SA discovered the system had been hacked. Hackers took advantage of the system's lack of security to make several international and premium number calls, amounting to a telephone bill of €12,208.71.

Normaction SA sent the bill to Fast Lease, alerted its client to the probable hacking of its PABX system and urged Fast Lease to change the password to avoid any further hacking. Fast Lease refused to pay the telephone bill, arguing that it had not made the calls that had led to the tremendous amount charged by Normaction SA as part of the telephone bill.

Normaction SA (now Nérim) filed a claim with the Commercial Court of Versailles in order to get Fast Lease to pay for the telephone bill. Fast Lease called AET Normaction (now UTT) into the case, concerning its liability for the system's lack of security, as it was the PABX system maintenance services provider.

The Court's ruling[1]

This ruling seems to take another step towards user protection in IT agreements and thus, imposes more thorough obligations on the service provider, especially regarding the duty to advise and inform users. First, the Court stated that ensuring the security of a system by changing the password is the responsibility of the user, as long as such user has been duly informed of the necessity to change the password and duly trained on how to do so.

In addition, the Court rejected Normaction SA's liability, stating that Fast Lease was solely liable for the calls originating from its network, and condemned the latter to pay the telephone bill.

However, the Court also considered that AET Normaction was liable as the maintenance services provider, by failing to warn its client about the lack of security of its PABX system and on the necessity to change the password, since: i. Fast Lease is obviously a layman in the telecommunications field; ii. AET Normaction declares that it is a specialist in the telecommunications field; iii. The maintenance services agreement provided for an obligation on AET Normaction to verify, on a yearly basis, the conditions and security of the equipment and system; and iv. The maintenance services agreement provided for a general obligation on AET Normaction to advise and inform Fast Lease, with regard to the services provided.

Therefore, the Court declared AET Normaction liable for failing to fulfill its duty to advise and inform Fast Lease under the PABX maintenance services agreement and condemned AET Normaction to repay all the sums charged by Normaction SA for the telephone bill.

Broader case law context

This ruling is similar to the ruling issued by the French Supreme Court on 2 July 2014[2]. In that case, a company entered into an agreement with a service provider for the rental of telecommunications equipment and the provision of telecommunications services, secured by an IT system. The security system was incompatible with the clients' internet access connection and led to the failure of the service. The clients filed a claim against the service provider requesting financial compensation and termination of the whole agreement. Although the service provider alerted its clients on the need to change their internet access connection as soon as it discovered the failure, the Supreme Court considered that the provider failed to fulfill its duty to inform and advise its clients. According to the judges, the service provider should have given to its clients "detailed and personalized information" on the service, with regard to their internet connection, prior to the

failure. These rulings seem to fit into an overall trend of the French Courts, which tends to widen the scope of the service provider's duty to advise and inform their clients. With regard to the Commercial Court of Versailles' 'password ruling,' one may consider that the Court takes the service providers' liability one step further as it considers that, as a layman, Fast Lease was not supposed to know the need for (and the way of) changing its PABX password.

Password responsibility

On one hand, we note that the Court excluded Normaction SA's liability, even though it provided the equipment to Fast Lease. On the other, the Court held AET Normaction liable as maintenance services provider for failing to warn its client about the lack of security of its password.

One may consider that, as a professional with clear understanding of the security of the equipment, Normaction SA should have been the one liable for not warning Fast Lease, upon installation of the equipment, that the system password must be changed on a regular basis in order to efficiently secure the system.

On the contrary, the Court considered that the maintenance services provider, which became aware of the system's lack of security after the hacking, is the one liable as it failed to identify such lack of security beforehand.

Negligence/layman behaviour

The ruling also highlights that the user was a car rental company with very limited knowledge of the telecommunications field. As a consequence, the Court came to the conclusion that Fast Lease should be considered a complete layman in this field, no matter the level of technical skills and knowledge required to use and change a password: "it explains the fact that it [Fast Lease] could have used its PABX system for 3 years without changing the password and without being aware that its system was at risk."

In other words, the Court highlighted the negligence of the maintenance services provider, which failed to alert its client to the system's lack of security. However, the Court did not seem to consider that the user itself might have been negligent, as it is commonly and widely recognised (not only in the telecommunications field) that a password consists of a combination of numbers and/or letters, kept confidential by the user for the purpose of securing access.

Indeed, one may question why Fast Lease has not been considered negligent for using such an obvious password for three years. Fast Lease might also have intentionally kept an unsecured password to facilitate its own access (or the access of its employees) to the system. If that was the case, Fast Lease may have contributed to its own damage and could have been declared partially liable.

Either way, the service provider in charge of the maintenance services of a system is, at least when stated in the agreement, under the obligation - as obvious as the security measures might be - to warn clients on each and every risk it may face, intentionally or unintentionally.

Conclusion

This decision also raises a series of questions about the provider/client relationship and liabilities. For instance, what would have happened if Fast Lease only rented the equipment and subscribed to the telephone service, without entering into the maintenance agreement with AET Normaction? Would it have been considered solely liable for the lack of security? What is the extent of the service provider's duty to provide information and advice, regarding security measures? Should they regularly verify password security? How frequently should they remind their users to change their passwords? Should they impose criteria for passwords to ensure they are secure enough?

In the information society we live in, where passwords are used to secure access to credit cards, computers, mobile phones and online accounts, to what extent can one be considered layman enough, not to know how to use a password efficiently? These questions will have to be addressed by the French Courts, in order for service providers to ascertain what level of technical knowledge they can expect from their clients.

In the meantime, we note that the overall trend of the French Courts is moving towards a more protective case law framework for users, which must be taken into account by service providers when contracting and dealing with clients. As the risk of cyber attacks and hacking increases every day, IT services users (including internet users) appear to be helpless targets. It seems that passwords are usually breached because of human weakness, not due to sophisticated technologies. Therefore, service providers, especially those delivering online services must, not only prepare for such threats, but they also must anticipate the carelessness of their own clients.

Laurie-Anne Evra-Ancenys Attorney
Almamy Touré Attorney
Gide Loyrette Nouel, Paris
ancenys@gide.com
almamy.toure@gide.com

1. Commercial Court of Nanterre, 3rd Chamber, judgment of 5 February 2015, n°2013F00738.
2. Court of Cassation, 2 July 2014, n°13-10076.