CCTS
COMMISSIONER FOR COMPLAINTS FOR TELECOMMUNICATIONS SERVICES

Howard Maker
Commissioner
P.O. Box 81088
Ottawa, Ontario
K1P 1B1
1-888-221-1687
[redacted]

June 17, 2010

[redacted]

[redacted]

Re: CCTS Complaint #04-02-02-00022205

On April 1, 2010 we issued a Recommendation regarding this complaint. [redacted] accepted the Recommendation. We did not hear back from MTS Allstream ("MTS") so we contacted it. It advised us on April 30, the last day for response to the Recommendation, that it did not accept the Recommendation and that it was collecting the information necessary to provide a complete reply. We provided MTS with an extension of time to reply. MTS replied by letter dated May 13, 2010, confirming that it did not accept the Recommendation and providing its reasons.

Background

[redacted] complained that in March 2009 it received a bill from MTS, its business long distance service provider, recording charges for hundreds of long distance calls made in February 2009 (primarily to Bulgaria) which it claimed that it did not make. MTS sought to collect $64,897 in respect of these calls, which it confirmed had been made by hackers who committed long-distance toll fraud through [redacted] private branch exchange ("PBX") equipment. [redacted] position is that it took reasonable steps to secure its telephone equipment (using a professional telecommunications provider to install and secure its PBX). MTS disclaimed responsibility for the charges on the basis that the PBX equipment that was breached belongs to [redacted] that MTS does not maintain or support it, and that it is the customer's responsibility to ensure that its equipment is secure. MTS also noted that it has no obligation to monitor its customers' long-distance calling activity.

During the course of these proceedings MTS offered to resolve the dispute by providing [redacted] with a credit of $36,207, leaving [redacted] responsible for paying the balance. [redacted] declined the offer.

Recommendation

On April 1, 2010 we issued our Recommendation to the parties. In summary, we concluded that in the absence of information from MTS that we had been requesting since October 2009, we could not conclude with any certainty whether the breach had occurred through [redacted] PBX. We then examined MTS' Terms of Service – Small Business, which constitutes the contract between MTS and [redacted] to determine what it provided in respect of liability for these charges. We wrote:

We therefore examined the Terms of Service that governed the parties to establish the liability for these long distance calls. MTS' Terms of Service – Small Business... are open to interpretation as to the customer's liability for charges incurred as the result of unauthorized usage of the service.

MTS' position is that the customer is responsible for all charges made from its equipment. This is consistent with MTS' Unregulated Terms of Service for consumer customers (underlining added), which state:
"7.1 Customers are responsible for paying for all calls originating from, and charged calls accepted at, their telephones, regardless of who made or accepted them, including all applicable service and usage charges associated with such calls."

However, its Terms of Service for business customers (underlining added), such as [redacted] were different. The relevant provisions are:

4.3 The Customer shall be responsible for Customer's and User's use of the Services and Content."

The term "User" is defined:

"1.0 "User" means any person the Customer permits to access or use the Services.

The use of differing terminology in the consumer and small business Terms of Service persuades us that it was MTS' intention that these provisions be different. The difference, in our view, is that the consumer customer is responsible for the cost of all calls made from their equipment. However the small business customer is responsible only for the calls it makes as well as any calls it "permits" or voluntarily allows to be made on its line. Any other interpretation would render the different language used in the two sets of Terms meaningless.

There is no evidence that [redacted] gave permission to the hackers to make the calls in dispute.

Based on this analysis we recommended that MTS waive all of the disputed long distance charges, including taxes, late payment penalties and any other related charges.

MTS' Objection

MTS' May 13 letter is eleven pages long and is accompanied by a number of attachments. The letter provides much of the information we had been requesting since October 2010, and also corrects some of the misinformation provided by MTS earlier in the process.

In summary, MTS' position on the facts is that:

- There can be no doubt that the breach took place through [redacted] equipment;

- It is not possible that the hackers gained access through MTS' network;
- It is not possible that the fraud took place through some other mechanism, e.g. "clip on fraud"; and
- [redacted] had vulnerable long distance and voice mail passwords of only four digits in length.

In addition, MTS disagreed with our interpretation of the liability provisions of its Terms of Service. Its position is that a customer can permit access to the network either voluntarily or involuntarily. In this case, [redacted] failure to properly secure its network afforded the opportunity for the fraud to occur. Thus [redacted] permitted the hackers to access the service. The definition of "user" is any person the customer permits to access or use the service. The term "permit" in its ordinary meaning is "to afford opportunity or possibility". In MTS' view, [redacted] involuntarily permitted the hackers to use the service and therefore should be responsible for the cost of the calls made as a result.

Our Analysis

We appreciate MTS providing a response that includes much of the substantive information that we did not have from it when we wrote the Recommendation. For the purposes of this Decision, we are prepared to accept that the toll fraud took place through [redacted] PBX and not through the public portion of the network for which MTS would be responsible. We thus also accept that no clip on fraud or other methodology was employed. We are, however, not prepared to accept MTS' submission that [redacted] passwords were vulnerable simply because they consisted of four digits. While common sense dictates that the larger and more complex the password the more secure it is likely to be, no evidence has been provided that the passwords used by [redacted] were factory defaults, simple combinations (e.g. 1234), or easily guessable combinations (like a date of birth). In addition, MTS has provided no evidence to show that four-digit passwords were considered to be below "industry standard" at the date of the breach in question. Ironically, along with its response MTS provided documents from Subex Limited (a global provider of Operations and Business Support Systems to communications service providers) and from Nortel (among other things, a PBX manufacturer).

Both documents discuss the manner in which PBX breaches can occur and the steps that businesses can take to avoid becoming victims. Both documents discuss the need to secure passwords, and to change them frequently. Neither document discusses password length and neither indicates that a four-digit password, in and of itself, is substandard or constitutes a failure to properly secure a PBX system. It is also worth noting that both of these documents describing safeguards against PBX hacking were dated "2009" and were likely released after the events at issue here, which occurred in February 2009.

In our view, this case still turns on the interpretation of the MTS Terms of Service. Even if we accept that the fraud occurred through the [redacted] BX, we cannot impose liability for the charges on [redacted] unless it is clear from the "contract" governing the relationship between the parties that liability is intended to flow in this manner.

On this issue we remain struck by the difference between the consumer Terms and the Business Terms. It is completely clear from the consumer Terms that on these facts the customer would be responsible for the losses (*"7.1 Customers are responsible for paying for all calls originating from, and charged calls accepted at, their telephones, regardless of who made or accepted them, including all applicable service and usage charges associated with such calls."*). It is clearly the intent of the drafter that consumers are responsible for all calls to or from their telephones, without exception. The Business Terms are different, and as the drafter, in our view MTS bears the responsibility for any lack of clarity or ambiguity. As previously discussed, the Business Terms make the business customers liable for the use

of the service by the customer and by any "user", which is defined to mean anyone the customer permits to access or use the service.

In our view, the available information shows some reasonable efforts on the part of [redacted] to secure its system. To accept, as MTS suggests, that any involuntary act of [redacted] can also impose liability upon it is not consistent with the business Terms of Service and would render meaningless the difference between the consumer and business Terms. As the drafter of both sets of Terms, it was open to MTS to clearly and unequivocally impose this liability on its business customers as it does on its consumer customers. As it chose not to do so, we must respect this distinction and give meaning to it.

Decision

For these reasons, we see no basis to vary our Recommendation. Accordingly, MTS will waive all of the disputed long distance charges, including taxes, late payment penalties and any other related charges.

Further to the provisions of the Procedural Code, [redacted] may accept or reject this Decision within 20 working days. Should it decide to reject the Decision, it may pursue this complaint in any other forum and MTS will be fully released from the Decision. If it accepts the Decision, MTS is bound to implement its terms.

A copy of the Code is attached for ease of reference.

Sincerely,

Howard Maker
Commissioner

Enclosures: 1. CCTS Procedural Code

CCTS
COMMISSIONER FOR COMPLAINTS FOR TELECOMMUNICATIONS SERVICES

Philippe Mercorio
Investigator
P.O. Box 81088
Ottawa, Ontario
K1P 1B1
1-888-221-1687
[redacted]

April 1, 2010

[redacted]

RE: CCTS Complaint #04-02-02-00022205

We have completed our investigation of the complaint of [redacted] regarding fraudulent long distance calls appearing on its MTS Allstream (MTS) bill. We appreciate the patience of both parties during this lengthy investigation. Our investigation process exceeded its usual timeframe due to the complexities of this case.

The Complaint

[redacted] incurred long distance charges for hundreds of long distance calls that it did not make, primarily to Bulgaria[1], in February 2009. The amount of the bill dated March 22, 2009 is $64,897.89, virtually all the charges being for fraudulent calls. [redacted] reported this problem to the police. [redacted] states that its average long distance charges are $40.00 per month and it is not willing to pay the disputed charges as they are of a fraudulent nature. [redacted] also points out that MTS did not notify it of this fraudulent activity.

[redacted] says that it had taken reasonable steps to secure its telephone system prior to the occurrence of these fraudulent calls; each user had an assigned voicemail password and a professional company, [redacted] had been hired to install the telephone equipment and set up its security. In addition, long distance codes were also set up in order to place international calls. Furthermore, a record of all passwords was kept by the system administrator.

[1] A few calls were also made to Sao Tome & Principe and Zimbabwe

It is [redacted] position that it met all of its obligations and therefore that it should not have to pay any of these extraordinary charges.

MTS' Position

MTS notes that [redacted] reported being a victim of telephone PBX toll fraud on March 24, 2009 and that a hacker(s) was able to break into [redacted] voicemail system to place unauthorized long distance calls totalling $64,897.89. MTS states that it was not responsible for the maintenance or monitoring of [redacted] customer-owned PBX equipment. It was the customer's responsibility to ensure the adequate security of its PBX infrastructure in order to avoid becoming the victim of such fraudulent calls.

MTS does not provide customers with a fraud monitoring service associated with customer-owned equipment. Any network monitoring done by MTS is for internal purposes only and is not intended for the purpose of identifying a customer's unusually high long distance usage. If MTS notices unusual long distance activity, it may notify a customer of such a situation as a courtesy. Furthermore, all of [redacted] toll calls were carried on Bell's network[2]. MTS was therefore not in a position to detect the suspicious calling occurrences.

MTS continues to maintain that [redacted] is responsible for the outstanding long distance charges in the amount of $64,897.89. However, as a goodwill gesture, MTS has offered [redacted] a credit of $36,207.00 including taxes.

Analysis

MTS' analysis of the matter presumed that the breach took place through the customer's equipment. We asked MTS to provide us with the basis upon which it determined that the breach occurred through the customer's equipment and not through the public network, for which the customer is not responsible. MTS has provided the following in support of its position:

1. All the international calls were made through a voicemail whose password code 1234, a vulnerable code;
2. The customer's local service is provided by Bell and only the long distance calls are routed over MTS' network[3], which means that there is no way to access the customer's line from within MTS' network, and
3. If it had been a case of "clip-on fraud" (where a hacker physically attaches cables to the network facilities), only one line would have been involved and the concurrent calling and overall volume of calls seen in this case would not have been experienced.

Despite our requests for clarification, MTS has not explained how it claims to know that the password code used was "1234", a sequential and therefore weak password. We also noted that in some of its correspondence with CCTS, MTS claimed that all of [redacted] long

[2] It is our understanding that MTS uses Bell's network in order to provide its customers with LD service in Toronto, where it does not have its own network facilities.
[3] That statement contradicts MTS' previous comment that the LD calls were carried over Bell's network.

distance calls were carried on Bell's network, whereas in other correspondence it stated that they were carried on its own network. As for its statement that it was not a case of "clip on fraud", that conclusion is merely speculative, as MTS did not provide any indication that it conducted a physical examination of the facilities.

[redacted] stated that it had taken reasonable steps to secure its telephone equipment prior to the occurrences of the fraudulent calls; it hired a professional telecommunications company to install and secure its system, restriction filters were created and outbound transfer capabilities were disabled from all voicemail boxes. However, [redacted] also stated that the outbound calling restriction had one exception that allowed calls placed to [redacted] outside business hours to be forwarded to another number in case of emergency. [redacted] also confirmed that all of its long distance and voicemail passwords had only 4 digits at the time that the fraud occurred.

We are of the opinion that it is not possible to determine how the hackers accessed [redacted] system. The facts presented to us are inconclusive as to which end of the network the hackers used to gain entry: [redacted] or MTS'.

We therefore examined the Terms of Service that governed the parties to establish the liability for these long distance calls. MTS' Terms of Service – Small Business[4] clearly show that MTS had no contractual obligation to secure [redacted] telephone equipment or voicemail system, or to monitor long distance calling activity for the benefit of the customer. However, the Terms are open to interpretation as to the customer's liability for charges incurred as the result of unauthorized usage of the service.

MTS' position is that the customer is responsible for all charges made from its equipment. This is consistent with MTS' Unregulated Terms of Service for consumer customers, which state:

"7.1 Customers are responsible for paying for all calls originating from, and charged calls accepted at, their telephones, regardless of who made or accepted them, including all applicable service and usage charges associated with such calls."

However, its Terms of Service for business customers, such as [redacted] were different. The relevant provisions are:

4.3 The Customer shall be responsible for Customer's and User's use of the Services and Content."

The term "User" is defined:

"1.0 "User" means any person the Customer permits to access or use the Services.

The use of differing terminology in the consumer and small business Terms of Service persuades us that it was MTS' intention that these provisions be different. The difference, in our

[4] As they were at the time of the events. It should be noted that since the launch of CCTS' investigation, all of MTS' customers are now governed by the consumer Terms of Service.

view, is that the consumer customer is responsible for the cost of all calls made from their equipment. However the small business customer is responsible only for the calls it makes as well as any calls it "permits" or voluntarily allows to be made on its line. Any other interpretation would render the different language used in the two sets of Terms meaningless.

There is no evidence that [redacted] gave permission to the hackers to make the calls in dispute.

Recommendation

Based on our interpretation of the Terms of Service, we have no choice but to recommend that MTS waive all of the disputed long distance charges shown on the invoice of March 22, 2009, together with any related taxes, late payment fees and any other charges.

Attached is a copy of the CCTS Procedural Code which contains important information with respect to recommendations made by CCTS, including information about acceptance of recommendations by a complainant and a telecommunications service provider. In particular, we refer [redacted] and MTS to sections 10 and 11.

Sincerely,

Philippe Mercorio
Investigator

Enclosures