CCTS
COMMISSIONER FOR COMPLAINTS
FOR TELECOMMUNICATIONS SERVICES

HOWARD MAKER COMMISSIONER
[redacted]
P.O. Box 81088, Ottawa, ON K1P 1B1

April 17, 2012

[redacted]

[redacted]
MTS Allstream
333 Main Street
Winnipeg, Manitoba
R3C 3V6

Re: CCTS Complaint #171665

On March 20, 2012, we issued a Recommendation regarding the above complaint. As [redacted] rejected our Recommendation, I am required to issue a Decision under Section 11 of our Procedural Code ("the Code").

Our Recommendation

After investigating [redacted] complaint, we determined that:

- the security breach most likely occurred through [redacted] telephone equipment;
- MTS did not sell or install [redacted] telephone equipment;
- MTS was not responsible for the maintenance or security of [redacted] telephone equipment;
- [redacted] failed to take steps to secure its telephone equipment following a recent prior occurrence of fraudulent long distance calls, thus likely facilitating the improper access to its phone system; and
- MTS has advised that its offer to settle the complaint is based on covering its costs and that it will not profit from this fraudulent activity.

Accordingly, we recommended that the dispute be resolved on the basis of the offer by MTS to credit almost $18,000 of the $28,700 billed to [redacted] in connection with the fraudulent long distance calls.

[redacted] Objections

Under Section 11 of the Code, the party objecting to the Recommendation is required to explain why he or she considers it to be unacceptable or inappropriate. [redacted] provided its objections by way of a letter from its lawyers, MacDonald Associates, dated April 9, 2012.

[redacted] alleges that CCTS erred in formulating its Recommendation, as follows:

1. CCTS incorrectly interpreted material facts by stating that [redacted] did not implement any of the recommended restrictions to its telephone equipment following the first occurrence of fraudulent calls, when in fact it had done so; and
2. The Recommendation makes a "false interpretation" of MTS' Terms of Service.

Analysis of Objections

Implementation of Phone System Restrictions

[redacted] stresses that CCTS erred in saying that [redacted] had failed to implement appropriate restrictions on its phone system following the first episode of long distance toll fraud. It states that it changed all of its voicemail passwords from 4 to 6 digits immediately after the first occurrence of fraudulent calls, and it points out that this is reflected in an MTS call note. As such, [redacted] is of the opinion that it took reasonable steps to secure its telephone equipment.

Immediately following the first episode of toll fraud (which occurred in November 2010), MTS provided [redacted] with a two-page document called "Protect your PBX" (copy attached). This document contained a list of recommendations to be implemented by [redacted] in order to help it better secure its telephone equipment.

Among the recommendations featured in that lengthy list are the following:

- Restrict access to specific times (business hours) & limit calling ranges;
- Block all toll calls at night, on weekends and on holidays;
- Restrict call forwarding to local calls only;
- Block, limit access or require attendant assistance to overseas calls;
- Block or restrict overseas access;

- Use longer DISA (direct inward system access) codes (minimum 7-9 digits) and change the codes regularly.

[redacted] objection referred to it having implemented just one of these measures following the first occurrence of fraudulent calls, i.e. the increase in the number of digits in its voicemail passwords. We also noted that in its email to CCTS dated February 27, 2012, [redacted] acknowledged that "nothing was blocked at the time of the hacking".

The reason that this list of recommended security measures is so lengthy is that fraudsters are capable of breaching a telephone system through many different paths. While increasing the number of digits in passwords is appropriate, it is just one measure available to customers to protect their phone systems from unauthorized access. It is for this reason that a multi-dimensional approach to system security, as outlined in the MTS documentation (and in numerous other documents easily found on the internet) is strongly recommended. In summary, the evidence in this case falls short of persuading me that, in the circumstances of this case, [redacted] took reasonable measures to secure its system.

MTS' Terms of Service

[redacted] takes the position, in the alternative, that even if CCTS finds that [redacted] did not adequately secure its phone system, that it cannot be held liable for an "involuntary" failure to secure its system. [redacted] points to the language of MTS' Terms of Service, as well as the language used in a previous CCTS Decision, to support the argument that [redacted] should not be held liable when it allowed access to its system to fraudsters, when it did so through conduct that was involuntary.

MTS' Business Terms of Service provide:

"The Customer shall be responsible for Customer's and User's use of the Services and Content". "User" is defined as "any person the Customer permits to access or use the Services". [redacted] contends that since there is no evidence that it "gave permission" to the fraudsters to make calls through its system, it should not be liable for them. It points to language in the prior Decision in which CCTS explained that a service provider's Terms must clearly impose liability on a customer if it wishes to rely on them.

We maintain the position that liability is not to be imposed on customers absent clear language to that effect in the Terms. The question then is whether [redacted] "permitted" the fraudsters to access its system.

I do not think it reasonable to characterize [redacted] conduct, which facilitated access to its phone system, as "involuntary". It suffered an incident of toll fraud in November 2010. It received advice from MTS on how to prevent future occurrences. For whatever reason – it did not implement these changes. In my view, particularly in the circumstances, this was a voluntary omission by [redacted], which was provided with the necessary information and chose not to implement these safeguards. By using the term "involuntary", [redacted] suggests that there was nothing it could have done to protect against the long distance fraud at issue in this complaint. Although that was the case in the prior Decision on which [redacted] relies, it is quite clearly not the case here. [redacted] made an informed, voluntary choice, not to implement the recommended security measures.

For these reasons, I conclude that [redacted] "permitted" the thieves to access its system by failing to take the necessary steps, of which it was fully aware, to secure its system. Accordingly, I see no reason why MTS should not be able to rely on its Terms of Service.

Decision

Section 11.5 of our Procedural Code provides that in formulating a Decision the Commissioner shall consider whether there is substantial doubt as to the correctness of the original Recommendation. In my view, [redacted] has failed to demonstrate doubt as to the correctness of the Recommendation.

Further to Section 11.7 and 11.8 of our Procedural Code, [redacted] may accept or reject this Decision within 20 days of receipt. Should it decide to reject this Decision, [redacted] may pursue this complaint through any other forum and MTS shall be fully released from the Decision. A copy of our Procedural Code is attached for reference.

Sincerely,

Howard Maker
Commissioner