PABX FRAUD

Customer Awareness Pack

PABX Fraud | Jan 2016

IT'S HOW
WE CONNECT

Pack Contents

Slide 3	**What is PABX Fraud?**
Slide 4	**How and why Fraudsters try to access your PABX service?**
Slides 5-7	**What are the customer's responsibilities?**
Slides 8-9	**What is Telstra doing to assist in preventing and mitigating PABX Fraud?**
Slide 10	**Fraud prevention strategies**
Slides 11-12	**Frequently Asked Questions**

What is PABX Fraud?

The below is a short synopsis of PABX Fraud and does not cover all types of Telecommunication Fraud. Compromised PABX / Voicemail systems have been reported as a large fraud issue with nearly $5 billion losses globally each year.*

- Fraud is an industry-wide problem impacting businesses that own or operate their own Customer Premise Equipment (CPE), typically PABX or voicemail systems and more recently TIPT solutions.
- “Feature rich” systems offer functionality like direct inward system access (DISA) intended to enable authorised users, usually employees, to make calls billed to their company account while not on the premises. This increases an organisation’s vulnerability if appropriate preventative security measures are not in place. Hacked voicemail and email viruses are also responsible.
- Fraudsters know how to access these systems and make outbound calls domestically or internationally which, from a network perspective, appear to be legitimate and are billed to the compromised account.
- A fraud attack starts by the fraudster hacking into the system and then establishing call re-routing without the owner’s knowledge. Once established, subsequent incoming calls are re-routed within the system as outgoing calls to other destinations.
- Costs associated with CPE fraud can escalate very quickly in a short time frame.
- Fraudsters profit from this activity by selling calls for profit or calling Revenue Share Numbers and billing them to your account.
- More sinister beneficiaries of this fraudulent activity are terrorist organisations with evidence linking profits raised from CPE fraud to recent terrorist activities.

*Communications Fraud Control Association, 2011 CFCA Global Fraud Loss Survey, http://www.cfca.org/pdf/survey/Global%20Fraud_Loss_Survey2011.pdf

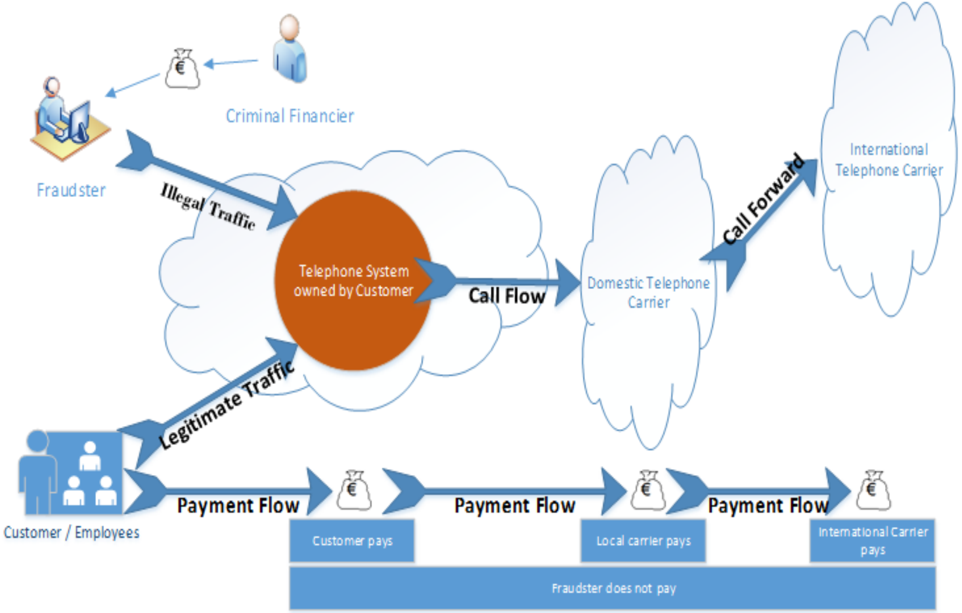
How and why do Fraudsters try to access your PABX service?

How Fraudsters access PABX service

An attacker tries different admin passwords to infiltrate a customer's telephone system. If they get access, they establish a call-forwarding or a dial-thru to a high price destination. After that the attacker originates many calls to the infiltrated telephone system, usually from an IP based source to avoid detection, and the system forwards the calls to the expensive destination. In some other cases, the attacker programs software which initiates calls automatically, avoiding the need to generate incoming calls.

Why Fraudsters access your PABX service

The core reasons why fraudsters abuse customers' equipment are many and varied but they come down to revenue raising. Fraudsters abuse customer equipment to raise funds for their own purposes, be it independent or organised crime. People conducting criminal activity may seek fraudulent pathways to conduct business that they don't want to be easily detected. International agencies allocate revenue specifically to detect, prevent and prosecute such activity.



IT'S HOW WE CONNECT

What are the customer’s responsibilities?

Customer Service Level Agreement (CSA) extract

1. This Agreement consists of the Service Schedules, these terms, any Attachments and Our Customer Terms formulated by Telstra for the purposes of Part 23 of the Telecommunications Act 1997 (Cth) (Our Customer Terms), including all amendments we make to Our Customer Terms after the date of this Agreement. If there is an inconsistency between parts of this Agreement, the Services Schedules will prevail, followed by these terms, any Attachments and then Our Customer Terms.
2. You acknowledge either receiving, or having had the opportunity to review, a copy of Our Customer Terms. You may view Our Customer Terms at http://www.telstra.com.au/customerterms/ or obtain a copy from us. If you require information about detrimental changes to Our Customer Terms before they take effect, it will be available on the above website.

Our Customer Terms General Terms for Small Business Customers

Your responsibility
3.6 You are responsible for and have to pay for any use of your service, whether you authorise it or not. Also, if you do not disconnect your service when you leave your premises, you have to pay for any use of the service by later occupants or others. We recommend you consider taking measures to protect yourself from unauthorised use of your service. Any person who uses your service, or allows someone else to use it, after you have vacated your premises, is jointly and individually liable with you for any charges relating to that use.

Excessive or unusual use
3.7 In some circumstances we may monitor usage of your service for excessive or unusual usage patterns, but we do not promise to do so.

Your responsibility for equipment
3.11 You are responsible for any equipment at your premises (including any that belongs to us). You have to pay us for any loss or damage to our equipment at your premises, except for fair wear and tear.

Telephone numbers and PIN's
11.4 Because you have to pay for any use of your service, whether you authorise it or not, we recommend you protect the security of any PIN used with your service.

*OCT are subject to change, for up to date information on OCT please go to http://www.telstra.com.au/customerterms

IT'S HOW WE CONNECT

Our Customer Terms General Terms for Corporate Customers (Large Business and Government)

Your responsibility

3.6 You are responsible for and have to pay for any use of your service, whether you authorise it or not. Also, if you do not disconnect your service when you leave your premises, you have to pay for any use of the service by later occupants or others. We recommend you consider taking measures to protect yourself from unauthorised use of your service. Any person who uses your service, or allows someone else to use it, after you have vacated your premises, is jointly and individually liable with you for any charges relating to that use.

Excessive or unusual use

3.7 We do not promise to monitor your service for excessive or unusual usage. We can suspend or cancel your service if it is used in an excessive or unusual way, but do not promise to do so. If we do suspend or cancel your service, you still have to pay any charges incurred for any excessive or unusual usage.

There might be excessive or unusual use if you have a call that remains connected for an unusually long period of time or where an unusually large volume of calls to premium-rate or international services start being made from your service.

Your responsibility for equipment

3.11 You are responsible for any equipment at your premises (including any that belongs to us). You have to pay us for any loss or damage to our equipment at your premises, except for fair wear and tear.

Telephone numbers and PIN's

8.4 Because you have to pay for any use of your service, whether you authorise it or not, we recommend you protect the security of any PIN used with your service.

*OCT are subject to change, for up to date information on OCT please go to http://www.telstra.com.au/customerterms

IT'S HOW
WE CONNECT

What is Telstra doing to assist in preventing and mitigating PABX Fraud?

Fraud Identification routines

The Telstra Network Fraud Team run daily routines to detect suspicious international calls and unusual call patterns.

The routines detect suspect fraudulent behaviour by scanning:

- Common overseas destinations and phone numbers known to be used in PABX fraud
- Countries with a history of revenue share fraud and calls to popular numbers used to test hacks
- Previously blocked/unallocated revenue shared country call codes
- Calls being made to hot test numbers
- Review, validation and action of automatically generated TIPT alerts
- Proactive blocking of IDD calls from the customers A number to mitigate further financial impact to the customer
- Proactive block of IDD calls on the Network to cease calls being made to specific B numbers (destination)
- Notifications from Fraud Detection Database used to automatically generate suspect calling patterns to all countries
- Attendance of World Fraud Forums to keep abreast the latest Fraud trends globally

Alerts

The Network Fraud Team will send a SUSPECT FRAUD ALERT email to the customers Service Management Representative (SMR), their Group Manager (GM), and/or the Account Executive (AE) with details of the suspicious international calls or unusual call patterns. The Telstra customer representative will then forward the SUSPECT FRAUD ALERT to the customer directly to notify of the suspicious calls/unusual call patterns.

The email will include, but not limited to the following incident report information:

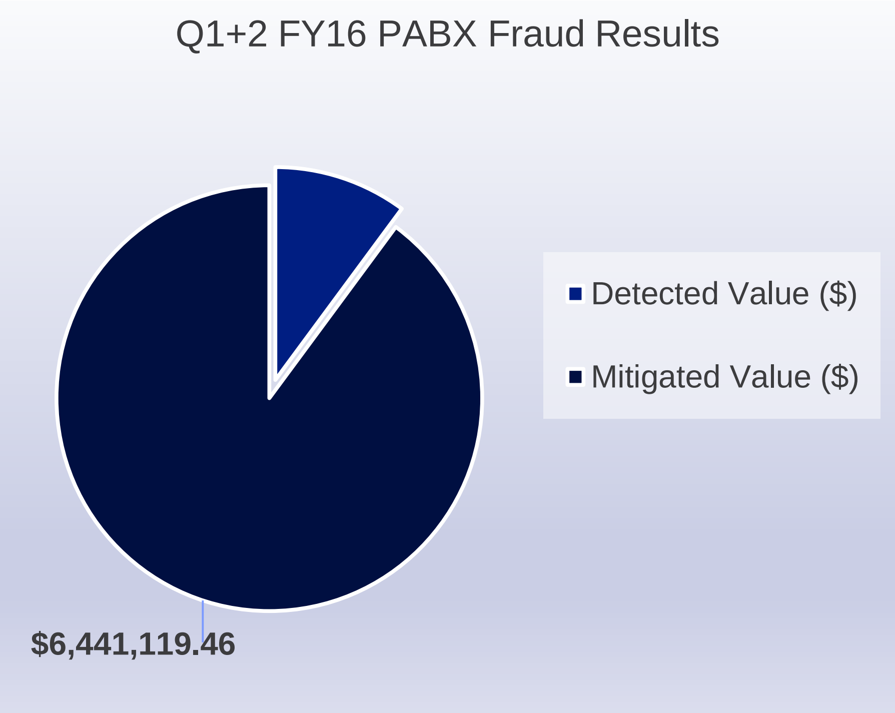
- Customers name, CIDN, Account, and Service numbers
- CSI reference number
- List of suspect countries dialled
- Services the calls entered the CPE on (if known)
- Services the calls left the CPE on (if known)
- Number of calls made
- Date the calls started
- Records of previous hacking incidents
- Resources to help you talk to your customer about CPE fraud, including:
  - CPE Fraud Management and Processes.
  - PABX Fraud Frequently Asked Questions

IT'S HOW WE CONNECT

Mitigating PABX Fraud Data

The Network Fraud Team identified 334 PABX/TIPT hacks in Q1+2 FY15/16, with a mitigated amount of $6.4M.

The mitigated value is calculated based on the time between when the fraudulent calls ceased (as a result of the Telstra Network fraud team blocking the calls on the network) to when the customer's next bill is issued and analysed; where the increased call volumes would typically be identified by the customer and are ceased after making the required security changes to their privately owned/managed equipment. These calls would have continued should the call patterns remained unchanged and the Telstra Network Fraud team not intervened.



IT'S HOW WE CONNECT

Fraud Prevention Strategies

Below are examples of some fraud prevention strategies customers can implement to reduce the likelihood of being a victim of fraudulent activity.

- Make sure someone familiar with the customer's billing and normal calling patterns reviews your account on a regular basis.
- Most systems now generate traffic monitoring logs in real time as standard or an additional add on. Monitor these so you can be aware of fraud before receiving your bill.
- Do not allow your system administrator to maintain factory-set passwords.
- Introduce a PIN and password management policy that:
    - does not allow "weak" PINs (1234, 1111, 0000, first or last four digits of their phone number)
    - includes regular PIN changes when an employee or contractor leaves the business
    - discourages employees from posting access codes and passwords in plain view.
- Ensure your system room is locked when not attended and do not allow unauthorised access.
- Protect against "dumpster-divers" by securely disposing of documents which may contain employee names, phone numbers, access codes etc.
- Consider your business needs and if appropriate blocking access codes for external dialling, special prefix codes (enabling calls to be carried over another network such as Optus, Vodafone etc. which will not be visible to Telstra), flexible feature codes and restrict international calls.
- Restrict call forward features so that extensions cannot forward calls to long distance.
- Develop a Fraud Emergency Response plan with your supplier so you know what to do in the event of a fraud attack.

FAQ’s

Is this fraud widespread?

Fraud is an ongoing issue. Any customer with poor PABX or Voicemail security is potentially a target. Customers need to regularly audit their systems and ensure security is up to date. This is does not just affect Telstra. It is an industry wide issue.

How often has it been detected?

On average, Telstra identify between 50 and 60 customer services a month who have been affected by PABX/Voicemail fraud. The amount of money involved varies but can be significant.

Are customers eligible for a refund?

This is fraud perpetrated on customer private equipment. As a result the customer is liable for costs incurred.

How can Telstra tell if the calls were fraudulent?

When Telstra identifies an issue, it will advise the customer. The customer then investigates their call records and determines if the calls are fraudulent. Telstra perform analysis on all International call detail records (CDR’s) cross referencing them with multiple Fraud databases containing known Fraudulent numbers. Refer to slide 8 for additional tasks carried out by the Telstra Network Fraud team to mitigate fraudulent calls from being made.

Has Telstra notified the police?

Telstra Corporate Security is in regular contact with federal agencies such as the Federal Police, High Tech Crime Unit and this issue has been identified as a problem. However, ultimately the responsibility rests with the customer.

Is there any way Telstra can track the calls?

We are empowered to collect relevant call records in order to analyse events without compromising privacy obligations. Calls originating from other countries do not normally provide originating calling number information. Information is not sent between international carriers.

What has Telstra done to rectify the problem?

This is an issue with customer equipment, so it is important that a customer's system is secure. Telstra recommends customers undertake regular security audits of their telecommunications equipment, such as PABX, Voice Mail platform, Voice Mail boxes or call queuing systems. Telstra will perform call blocking on the Network to ensure suspected fraudulent calls cease immediately reducing the operational and financial impact to the customer.

Will this impact the Telstra Home Messages service?

No. This fraud relates to customer equipment such as PABX, Voice Mail platform, Voice Mail boxes or call queuing systems.

Is it up to the customer to do something or can Telstra fix this issue?

Customers should ensure they are vigilant regarding their security. They can conduct a telecommunications system security audit as outlined above.

Can you access customer messages through this fraud?

Yes, fraudsters can access messages left on the voicemail box if they have fraudulently discovered the customers PABX PIN number.

What should customers do if they think they have been a victim of this fraud?

Contact their equipment maintenance organisation. If they confirm they have been the victim of fraud, the Police should be contacted immediately.

Who should I contact should I suspect I have been the victim of PABX Fraud after reviewing my bill?

Global Enterprise and Service and **Telstra Business** customers, please contact your Telstra Service Manager and/or Telstra Account Executive who will coordinate and facilitate an investigation to confirm whether you have been the victim of PABX fraud.

Small Business and **Consumer customers**, please contact the Telstra Front of House Billing Disputes team who will coordinate and facilitate an investigation to confirm whether you have been the victim of PABX fraud.

THANK YOU

IT'S HOW
WE CONNECT