Vandercom Fraud Protector

Every business with a telephone line is a potential target for telecoms fraud or misuse, whether that is by external hackers or internal users. Businesses that are IP-enabled or with telephone systems offer a larger opportunity for hackers to route calls through the system by methods known as dial-through fraud.

External hacking has become more sophisticated with hackers able to automate the dates and times of dial-through fraud to happen outside of standard working hours which allows them to go undetected by users on site. The victim will often be unaware of the breach until they receive their bill at the end of the month resulting in bill shock. However, the issue is not only limited to hacking with cases of staff misuse adding to the challenge, and ultimately the financial liability for fraud and unauthorised usage remains with your business.

Global losses attributable to telecoms fraud are estimated at US$29.2bn annually.
Source: CFCA 2017 Global Fraud Loss Survey
The UK is the 3rd most prevalent country for the origination of fraudulent calls.
Source: CFCA 2017 Global Fraud Loss Survey

What is Vandercom Fraud Protector?

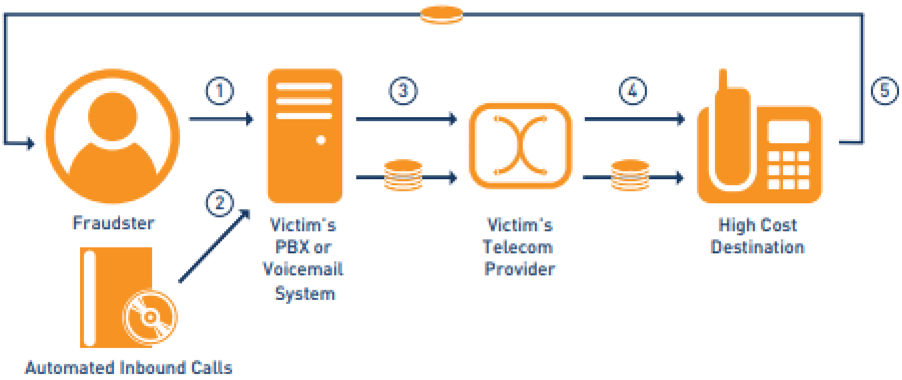
Vandercom Fraud Protector is a service provided to monitor, alert and protect customers from unnecessary financial exposure to telecoms fraud. Our staff and systems monitor call traffic in many ways including high value calls, high call volumes or high risk call types and known blacklisted numbers and destinations. On these occasions the calls are analysed and the customer is notified of any suspected fraud being committed on your telephone lines. In order to further help protect its customers from the risk of telecoms fraud, users of this service will also have their exposure to fraudulent calls limited to a maximum of £500 per line per day and often much less through early detection and action to suspend lines and bar calls. This unique call-fraud analytics system also offers you:

- The ability to limit your exposure to £500 of fraudulent calls per line per day

- Protection on your lines that are compromised or are suspected of being, with a dedicated team are ready to take action to suspend or, where possible, place specific call bars

Dial-Through Fraud (DTF)

There are many methods fraud can be committed but the most common is DTF. It is committed by the hacker compromising the PBX, Voicemail or individual extensions (1) and placing a divert on the user to a high value destination: this could be to high value UK numbers including 08, 07 and 09 numbers or International High Value (IRSF - International Revenue Share Fraud) destinations including Inmarsat calls costing in excess of £15.00 per minute (4). Once the call forward is in place, the hacker places multiple incoming calls to the compromised user (2) which results in the call being forwarded outside the PBX (3). The end result being that the customer is left with a large bill with the hacker receiving payments from the receiving network for the calls (5).



PBX dial-through fraud:

- Many telephone systems have external ports, enabling remote maintenance to take place
- Hackers can enter the PBX system through the port by using or breaking passwords
- Hackers can make calls through the PBX system, incurring call charge

Voicemail dial-through fraud:

- A hacker dials a number and goes through to voicemail
- A hacker enters the voicemail password
- This gives the hacker access to an outside line
- Hackers can now make calls through the PBX system, incurring call charges

How much is the service?

The service is charged on a per line basis based on the line type(s) as per the schedule below.

All charges are monthly in advance and exclude VAT. Please refer to the Terms and Conditions for the full details here: https://www.vandercom.co.uk/terms.html

Product	Monthly Rental (excluding VAT)
Single PSTN Line (per line)	£1.00
Multi line PSTN Line (per instance)	£3.00
ISDN 2 (per instance)	£3.00
ISDN 30 (per instance)	£10.00
UC Office Phone Connection (per connection)	£1.00

How does Vandercom Fraud Protector work?

Vandercom receives call data records from its suppliers 24/7 365 days a year at regular intervals throughout the day. The platform collects and imports this information and generates automated alerts which are analysed by our dedicated Fraud Team 24/7.

In addition to call pattern analysis the team shall be entitled (but not obliged) to automatically suspend any line that reaches or exceeds a daily spend limit of £500, or any other daily spend limit for that line which may otherwise be specified on the order form.