



**GOLDEN ORB NETWORKS**

# **White Paper**

## **Combating Telephony Based User Identity Fraud**

Prepared by: Stephen Bucklin, Chief Technical Officer, Golden Orb Networks Ltd

14 February 2011

**COMMERCIAL IN CONFIDENCE**

**Golden Orb Networks Ltd T: +44 020 8002 2422 E: [adrian.whitehouse@goldenorbnet.com](mailto:adrian.whitehouse@goldenorbnet.com)**

## Executive Summary

There is a growing problem in the financial services sector whereby phone calls from a bank, card provider, insurance company, or other financial institution with consumers are being redirected to fraudsters own phones in various ways, particularly when querying suspect transactions or conducting phone based banking or payments.

The concepts described in this document are designed to increase confidence between financial institutions and their clients in two ways;

1. By using the SS7 signalling mechanism underpinning the handling of all voice calls to attempt to discover if the intended call recipient has redirected or forwarded their stated phone number to another destination unknown to the caller.
2. By using a separate channel outside of the actual call-path being used to validate the calls being made between the two parties, particularly where the consumer is using a mobile phone.

## Background

It is possible that a call to or from a financial organisation can be manipulated in a number of ways to trick the financial institution's call centre into believing that it is a valid customer at the other end of the connection, where in reality, it is a fraudster. These attacks can manifest in a number of ways:

1. The fraudster calls the call centre and manipulates the customer number so that the CLI appearing on the contact centre screen appears to be correct even though the call is being placed from another device;
2. The fraudster calls the customer's phone service provider and poses as the customer who has lost their phone, and requests a call forward to another device. This means that any call from the bank or other financial institution is routed directly to the fraudsters phone without them knowing;
3. The fraudster calls the customer phone provider and again poses as the customer who has lost a mobile. This time they request a new SIM be provided to a new address. This allows the fraudster to gain full access to the customers mobile phone;
4. Network fraud. This is committed at the call centre servers, or at the VoIP provider supplying call centre telephony services. A 'hook' is used to detect an outgoing call to a customers mobile phone, and divert that call to another destination – typically the fraudsters mobile phone;
5. Premium call fraud. As in the previous case, but here outbound calls are "hooked" over to one of a number of premium rate lines with exorbitant charges that are billed back to the bank or financial company.

It should be noted that this area of technical fraud is only a single part of the overall risk of a transaction. A 'defence in depth' approach by the financial institution will cover other aspects, such as banking passwords, key phrases etc. It should also be assumed that the mobile operators have systems in place to stop many of these risks, however, these policies are out of the control of the financial institution.

This paper aims to discuss a number of methods in which additional security can be provided to validate the telephone connection between the financial institution and customer. There is no 'silver bullet' and any systems need to be used in conjunction with other security measures.

Any security measure needs to be balanced to allow ease of use for the customer, as making systems too cumbersome may alienate the customer and deter them from using the financial institutions telephone banking or payment systems. This may ultimately lead to customer dissatisfaction with the financial institution itself.

## Basic Concept

The basic premise in this paper is to explore two separate processes, both of which are designed to provide the financial institution with a greater level of confidence that the consumer they are conducting a conversation with over the phone is actually who they say they are.

### Signalling Data

One process is to use the SS7 Signalling underpinning the handling of voice calls to provide information back to the financial institute originating the call that the recipient has forwarded or otherwise re-directed their phone to another destination either inside or outside their home phone operators fixed or mobile network.

As a UK based Tier One phone operator, Golden Orb can process calls passing through it's secure network and use the signalling responses particularly from the recipient's mobile phone operator to identify if the recipients phone is being redirected or forwarded elsewhere. It can then pass this information back to the financial institution in a variety of ways to let them decide whether to proceed with the call, or use additional security processes to authenticate the call recipient in a number of ways.

### Separate Connection Paths

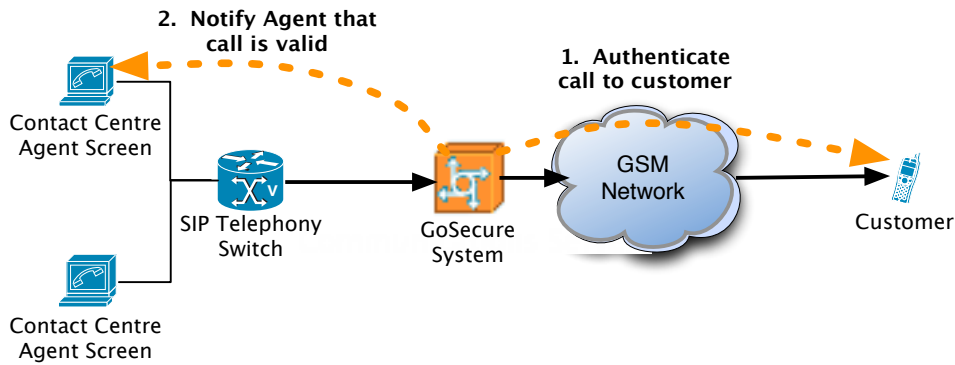
One such means of call recipient 'authentication' is by means of a separate connection path. This is similar to many security systems, such as encryption, where a 'key' or pass phrase is sent to the user by a different medium than the call. An example of this is Internet banking, where the initial password is sent by post to the consumers, who then enter these details to authenticate themselves on a secure web page.

The consumer's mobile phone can be reached by several completely separate methods. Historically, the voice path, the SMS (text) path, and the data path are all delivered to the mobile phone by different systems. Text paths are set up on different platforms, and are not a controlled (legislated) service such as voice and voice interconnections.

Data is rapidly becoming a main stay in the mobile market, but still presents difficulty, as many customers have different mobile instruments and differing levels of expertise of the user tends to limit the use of data services. Text, on the other hand, is universal and will work with all known instruments, and requires a very low user knowledge to *receive* a text.

The key concept here is to automatically authenticate a call using the text and voice paths to give a very high assurance that a financial institution is interacting with a particular customer.

Figure 1 below shows a simplified concept of operation. When voice calls are made between the customer and the financial institution agent, the GoSecure service will attempt to authenticate that the customer is actually using the mobile handset that is indicated to the financial institution agent (either incoming or outgoing).



**Figure 1: GoSecure Call Authentication Process**

The agent will receive a notification on their screen as to the validity of the call, both in the sense that the number being dialled is correct (ensuring the Financial institution’s SIP switch is not compromised) and that the mobile phone receiving the call is one being dialled and that the call is not being forwarded or re-directed elsewhere.

## Authentication

Any standard mobile instrument is capable of voice calls, and in addition has a limited and separate data path to the mobile operator. This data path is not the traditional IP data, but extra bits used in the network signalling paths. This connectivity has been utilised for two services:

### SMS

A Short Message Service Centre (SMSC) is designed to use this data path. A message is received by the SMSC (of limited length - larger messages are made up of a number of these messages) and the SMSC then uses the limited data path to attempt a connection to the mobile instrument. If the connection is successful, the message is transmitted to the instrument and deleted from the SMSC. Should the mobile not be found, the message will remain with the SMSC, and another attempt will be made later. Generally, should there be no success in reaching the mobile within two days, the message is abandoned. This system operates on a 'store and forward' basis. Most importantly, the SMS path is not affected by call diverts and other routing rules applied to the voice path. In addition, there is generally no way at present to withhold an SMS sending number.

### USSD

Unstructured Supplementary Services Data also uses this data path, but does not use an SMSC. Hence data is passed between the mobile instrument and the USSD server in real time as a session. Unlike SMS, should the phone be unavailable or out of service USSD is not possible. This service is used for many things such as top up balance, call divert requests and the like. A major advantage is that it is two way, and can accept responses from the mobile instrument. In the same way as SMS, this service is unaffected by any voice configuration.

The simple principle of an authentication is to send a PIN or phrase via USSD or SMS and have the recipient enter this on the telephone keypad, hence passing that back *via the other path (voice)*. If the sent PIN is authenticated with the received data from the user, it is a ***very high*** probability that the financial institution's agent is connected to the mobile instrument listed.

There are a number of ways of implementing this authentication, and these principally depend on the nature of the financial institution call centre. This is covered below in 'Call Set-Up'.

## Call Set-Up

Call set up is carried out between the financial institutions call centre and the Golden Orb core network. This will depend on discussion with the financial institution and the nature of the calls. There are a few different options:

### **Set up from the financial institution to the customer.**

This can be a data message generated by an agent by a web style button, or just a phone call to that customer via the GoSecure platform. This causes the GoSecure system to call the customer and uses the SS7 signalling response to indicate whether the call is being redirected or forwarded.

Where this is not possible, for whatever reason, the call recipient is invited to enter the PIN that will appear on the screen (USSD). Upon authentication, the call is connected directly to the call centre agent. Busy or unavailable customers will be responded to via a data message for display on the screen, should the initial set up be via a web button;

### **Set up from the customer to the financial institution**

**The** customer calls a number from their mobile phone. This causes the GoSecure system to invite them to enter the PIN that will appear on the screen (USSD). Upon authentication, the call is connected directly to the call centre agent. Alternatively, the call can be forwarded to the agent, and the agent can ask the customer to tell them the PIN on the mobile screen (This having been transmitted from GoSecure to the agent in advance of answering the call;

Set up from the financial institution to the customer can be again in the form of a data message generated by an agent by a web style button. This causes the GoSecure system to SMS the customer and invite them to call a number and enter a PIN. Both the number and the PIN are transmitted in the SMS. Upon GoSecure receiving the call with the correct PIN, the call will be forwarded to the call centre. The PIN can be valid for a specific time allowing the customer to make the call at their convenience;

The nature of the authentication needs discussion with the financial institution, and will be dependant on the reasons for the contact call.

## System Limitations

It is important to understand that there is no “silver bullet” with security, and this system should be used in conjunction with other security procedures to minimise the risk of fraud.

Using SS7 Signalling processes to determine if a particular consumers phone is being redirected elsewhere is dependant on the consumers phone provider providing a suitably detailed response to the voice call handling process, particularly when a call is being directed to them from another voice provider such as Golden Orb.

Whilst most major landline operators such as BT and others provide a suitable response across the SS7 Signalling layer indicating if the intended recipients voice call is being redirected or forwarded elsewhere, as of February 2011, a proportion of UK mobile operators do not and therefore this type of authentication process is of limited use.

It would be extremely useful if the relevant mobile operators could be persuaded to present the SS7 signalling responses, but it will take some concerted lobbying of the industry as a whole to achieve this. However, recent indications that some UK mobile operators would like to provide mobile payment services in some form presents an excellent opportunity for the financial services companies to put pressure on them to comply with the existing standards for voice call handling.

Authenticating call paths using SMS/USSD will be ineffectual for landlines, as SMS services are limited, and a digitised voice simply calls the number shown to ‘read’ the text. There is also no USSD service available (USSD is explained below). In addition, landlines can be forcibly ported by other operators without the use of a porting code meaning that there is no real security in the use of landlines.

Also, point three at the beginning of this document is hard to overcome. If a fraudster was able to have a replacement SIM sent, the authentication process will work. This point may be overcome depending on future access to mobile operator data. A new SIM may be issued with a new IMSI. If the IMSI of the original user can be logged, and then verified upon an authenticate request, it will be able to stop this fraud scenario.

## Conclusion

The use of Golden Orb's secure call management service (GoSecure) described here helps financial institutions combat a number of separate potential fraud attacks including;

- Inbound call spoofing from fraudsters appearing to call from the consumer's home or mobile phone number.
- Redirecting calls made from the financial institution to the consumers fixed or mobile phone to the fraudsters own number.
- Fraudsters or hackers comprising the financial institutions outbound call centre telephony system to divert inbound or outbound calls to their own phones or to a premium rate number.

We have designed a fully working test system as a proof of concept to highlight some of the potential solutions discussed within this paper. The site offers three separate scenarios of how both inbound and outbound calls can be authenticated and can be accessed through a standard web browser that can be used to manage calls between any fixed and mobile phones acting as the contact centre and consumer respectively.

Further details are available on request.