

Technical Disclosure Commons

Defensive Publications Series

October 2023

Establishing Phone Number Reputation Using a Contact Center Platform

Claus Regenbrecht

K Srinivas

Akiko Sexton

Follow this and additional works at: https://www.tdcommons.org/dpubs_series

Recommended Citation

Regenbrecht, Claus; Srinivas, K; and Sexton, Akiko, "Establishing Phone Number Reputation Using a Contact Center Platform", Technical Disclosure Commons, (October 18, 2023)

https://www.tdcommons.org/dpubs_series/6331



This work is licensed under a [Creative Commons Attribution 4.0 License](https://creativecommons.org/licenses/by/4.0/).

This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.

Establishing Phone Number Reputation Using a Contact Center Platform

ABSTRACT

Spam telephone calls decrease customer confidence in unknown callers; consequently, businesses can experience low call pickup rates. Some challenges with accurate caller identification are that a call from a legitimate business can be marked as spam, and that the name of the business that appears on the display need not be the actual owner of the number. This disclosure describes techniques to determine the accuracy of the caller ID and additional description such as business name or spam status reflected on a callee's mobile device. An outbound test call is initiated from a contact center platform to a test mobile device. The session screen of the incoming call displayed on the test device is recorded and sent to a database. The recorded session screen is validated against pre-recorded data. The validation establishes the accuracy of the displayed caller ID and determines if the call is tagged as spam, enabling the business to take corrective action as necessary.

KEYWORDS

- Trust provider
- Caller ID
- CNAM
- Spam call
- Dialer app
- Carrier telephony
- Automated dialing
- Call center

BACKGROUND

The increase in spam calls decrease trust among recipients when they receive calls from unknown numbers. Consequently, businesses experience low call pickup rates when reaching out to customers. Trust providers give callees more information about a calling number. For example, mobile carriers, phone dialer applications and standalone apps can mark calls as legitimate or suspicious. CNAM (caller ID name) is a feature in the public telephone network that identifies an incoming caller by a personal or business name associated with the calling party. However, these solutions are only available and effective in some countries. For example, CNAM is available only in a few countries. In countries without these options, it is possible for malicious actors to manipulate the caller ID to show local/regional and/or mobile numbers in such a way that the customer is misled into believing that a call is not spam.

Among the challenges with accurate caller identification are:

- Caller IDs can change their status over time;
- Caller ID information can be blocked or be missing;
- A service provider such as a mobile carrier or an application installed on a client phone can mark the caller ID as spam;
- Caller IDs can be made to appear as though they belong to a different business; etc.

Under these circumstances, a business owning the caller ID number has no visibility into the root cause of their low call pickup rates to identify suitable mitigating actions.

DESCRIPTION

This disclosure describes techniques to determine the accuracy of the caller ID and description reflected on a callee's mobile device. An outbound test call is initiated from a contact center platform to a test mobile device. The session screen of the incoming call displayed on the

test device is recorded and sent to a database. The recorded session screen is validated against pre-recorded data. The validation establishes the accuracy of the displayed caller ID and helps assess if the caller ID display is leading to a positive customer experience.

The outbound test call can be automatically dialed without manual intervention. Typically, a separate test platform is used to test call-center performance. The performance of the test platform sometimes may not correlate with actual production scenarios. The automated dialer can therefore be scheduled to initiate and establish a session between the far-end test mobile devices and the contact center platform actually used in production.

Fig. 1 illustrates techniques to establish phone number reputation using a contact center platform. A repository (A.1) includes test mobile devices of different characteristics and configuration, e.g., device model, country or region, operating system, mobile carrier, installed caller-ID apps, installed dialers, etc. The repository also includes caller IDs and business labels or trade names/brands used in the business context of the contact center. The repository can also include a database comprising numbers used in test environments.

A module (A.3) enables the selection of a test number, and another module (A.4) selects and assigns a caller ID to the test number. The selection of a test number and a caller ID can be done based on characteristics of test numbers and caller IDs/business names (as in repository A.1) that are of current interest.

A request for an outbound call can be initiated from a device (A.5) of a contact center agent, such as a desktop or a laptop. For example, the agent can initiate a session via a private branch exchange (PBX) or contact center platform (1.1), which establishes and maintains the session to mobile devices (4.1-4.3). The session is carried by a carrier (2.1), which can be a wired or wireless service provider operating on MPLS or Internet connection. The carrier can

interconnect to multiple other carriers (3.1-3.3) such as mobile service providers to establish the call to the mobile devices (4.1-4.3).

There can be multiple carriers connected to the contact center platform. While selection of the carrier does not determine the end test results, the selection of the mobile carrier does impact the results. The number used by user as caller ID may be displayed in different formats with each of the mobile carriers, since there is no standard on how the number is to be displayed. For example, the carrier systems in Fig. 1 (labeled 4.1, 4.2, 4.3) can display a number as “Anonymous,” “Likely Spam,” or just the number itself.

The test mobile devices are equipped with screen-grab (screen capture) applications (5.1) that capture the screen when a ring is generated on an incoming call. An OCR (optical character recognition) module (5.2) converts the captured screen to text that is sent to and stored (5.3) in a database (A.2). The database A.2 is a repository of data used in production environments. The captured text, e.g., caller ID, business name, description (such as ‘likely spam,’ etc.) is validated against the expected text as stored in the database (5.4).

Results are stored in the database as positive or negative based on the comparison between the screens captured on the test mobile devices and the expected text as stored in the database. A result is positive if the number and business label/description on the screen capture is the same as the true, assigned number and business label/description. A result is negative if the number on the screen capture is different from the true, assigned number, or if the number on the screen captured is flagged as ‘likely spam,’ ‘anonymous,’ etc.

As explained earlier, a customer support agent can initiate an outbound test call on a contact center platform to mobile devices under test to identify and validate the caller ID displayed, enabling the prediction of whether or not an actual production call is likely to have an

accurate caller ID. Supervisors, quality experts, and IT Operations personnel have the capability to initiate test calls to far-end test mobile devices for the purpose.

Alternatively, automated calls can be scheduled at periodic intervals, e.g., daily before the contact center opens, during break times, or at other times when human agents are not working, eliminating manual testing and reducing the turnaround times for issue resolution.

Fig. 2 illustrates an example workflow for establishing phone number reputation using a contact center platform. A contact center agent uses their device (e.g., mobile device, or, if using a desktop or laptop, a softphone) to connect to the contact center platform to initiate an outbound session to the far-end test mobile device. Session initiation can include the selection of a country (B.1) and the reserving of a remote test device (B.2.1) to initiate a test call through the contact center platform (B.3). Expected test results are set (B.5).

The call with the assigned number (B.2) establishes the session to the far-end test mobile phone (B.6). Once the call rings on the test device B.6 a captured screen (B.7) is pushed to a database and validated with expected results (B.8). For example, if the agent uses a caller ID 408-123-1234 to make a call to a test mobile device with number 987-654-3210, a screen capture displaying the caller as 408-123-1234 (along with any other text transmitted by the contact center such as an accurate business name or label) represents a positive (successful) test.

Positive test results (that match the expected results) are a signal that production calls can be initiated to mobile devices with profiles (e.g., device model, country or region, operating system, mobile carrier, installed apps, installed dialers, etc.) similar to the test mobile phone. If the displayed number is not 408-123-1234, or if other displayed text is other than what was transmitted by the contact center, or if the displayed text includes phrases such as ‘likely spam,’ ‘potential spam,’ ‘junk call,’ ‘possibly scam,’ etc., then the result is negative.

Fig. 3 illustrates an example screen capture (C.1) taken automatically at a test mobile device. The exact form of the screen capture depends on various factors such as the recipient's carrier; the caller ID application used; the operating system, make, and model of the test device; the number sent by the contact center platform; etc. For example, as illustrated in Fig. 3, the screen capture can include “Brand XYZ” as caller name/description and the caller ID (408-123-1234), or Brand XYZ and a phrase such as ‘likely spam,’ etc.

Fig. 4 illustrates an example method for an agent or automatic system to validate caller ID results. A call request is initiated with a specific number (D.1). The call initiated by the contact center platform triggers an outbound call session based on the selection of the far-end test number (D.2). The far-end test mobile device receives a call (D.3) and captures the screen of the event corresponding to the incoming call (D.4). The screen capture is pushed to a validation database (D.4). The results are validated with the expected caller ID and text (D.5). The test results are analyzed to determine if a production call can be placed or if corrective action is necessary.

In this manner, test calls to far-end test phones can be initiated from a contact center platform that is used in production. Caller IDs, as received by the test phones, can be fed back and analyzed for accuracy. Some salient features of the described techniques include:

Mobile device hardware of a variety of characteristics can be used for testing

The contact center platform used for production is the one that is used to initiate and terminate the session or call. To identify an issue (e.g., a legitimate caller being displayed as ‘spam’ or ‘suspicious’), the test setup replicates real (production), live scenarios for a specific country. To replicate a real scenario, mobile phones of a wide variety are deployed and remotely managed. The wide variety of mobile devices capture the range of caller ID display possibilities

presented by carriers, caller ID applications, operating systems, etc. Furthermore, test phones can be set up based on country-specific requirements, e.g., multiple mobile phone carriers for the country; multiple caller ID application providers; different mobile operating systems; etc. A test phone is registered in a database with their characteristics, e.g., in-country phone number, OS, make, model, installed caller ID applications, phone dialers, etc.

Test calls are made to mobile devices under test and the caller ID as displayed on the mobile devices under test is captured

A database of phone numbers, test mobile devices, and caller-IDs/business names is queried to select numbers and far-end mobile devices. An automated dialer or a human agent (using, e.g., a softphone) can trigger an outbound call with the selected caller ID to the test phone numbers. The outgoing call establishes the ringtone on the selected test devices. During the ringtone, caller ID details are captured and pushed to the database. The test can be performed with a specific carrier, application, or mobile operating system in a country. Based on the input selections, the test-matrix combination is populated, and the test calls are initiated, maintained, and terminated. When the test completes the numbers are released.

Display captured at the test mobile devices is compared with the expected display to determine the accuracy of caller ID, caller name, and caller description, and to identify problems with caller ID display

Once the results, e.g., the captured screenshots from test mobile devices, are received, these are validated for accurate reporting of caller ID, business name, etc. For example, a call from a business ‘XYZ’ that owns the number being displayed as a call from another business ‘ABC’ is an indication of a problem. The screenshot is used to determine if the call is tagged at

the callee's mobile device as spam. For example, the callee's display including phrases such as 'suspicious,' 'junk,' 'likely spam,' etc. is an indication of a problem.

Businesses and individuals rely on their phone calls being presented accurately to call recipients. The techniques described herein provide a single-platform solution that businesses can use to globally verify that their calls are identified correctly. The techniques enable businesses to take corrective action, such as reaching out to carriers, if their calls are misidentified, tagged as spam, or otherwise displayed to callees with incorrect information.

CONCLUSION

This disclosure describes techniques to determine the accuracy of the caller ID and additional description such as business name or spam status reflected on a callee's mobile device. An outbound test call is initiated from a contact center platform to a test mobile device. The session screen of the incoming call displayed on the test device is recorded and sent to a database. The recorded session screen is validated against pre-recorded data. The validation establishes the accuracy of the displayed caller ID and determines if the call is tagged as spam, enabling the business to take corrective action as necessary.

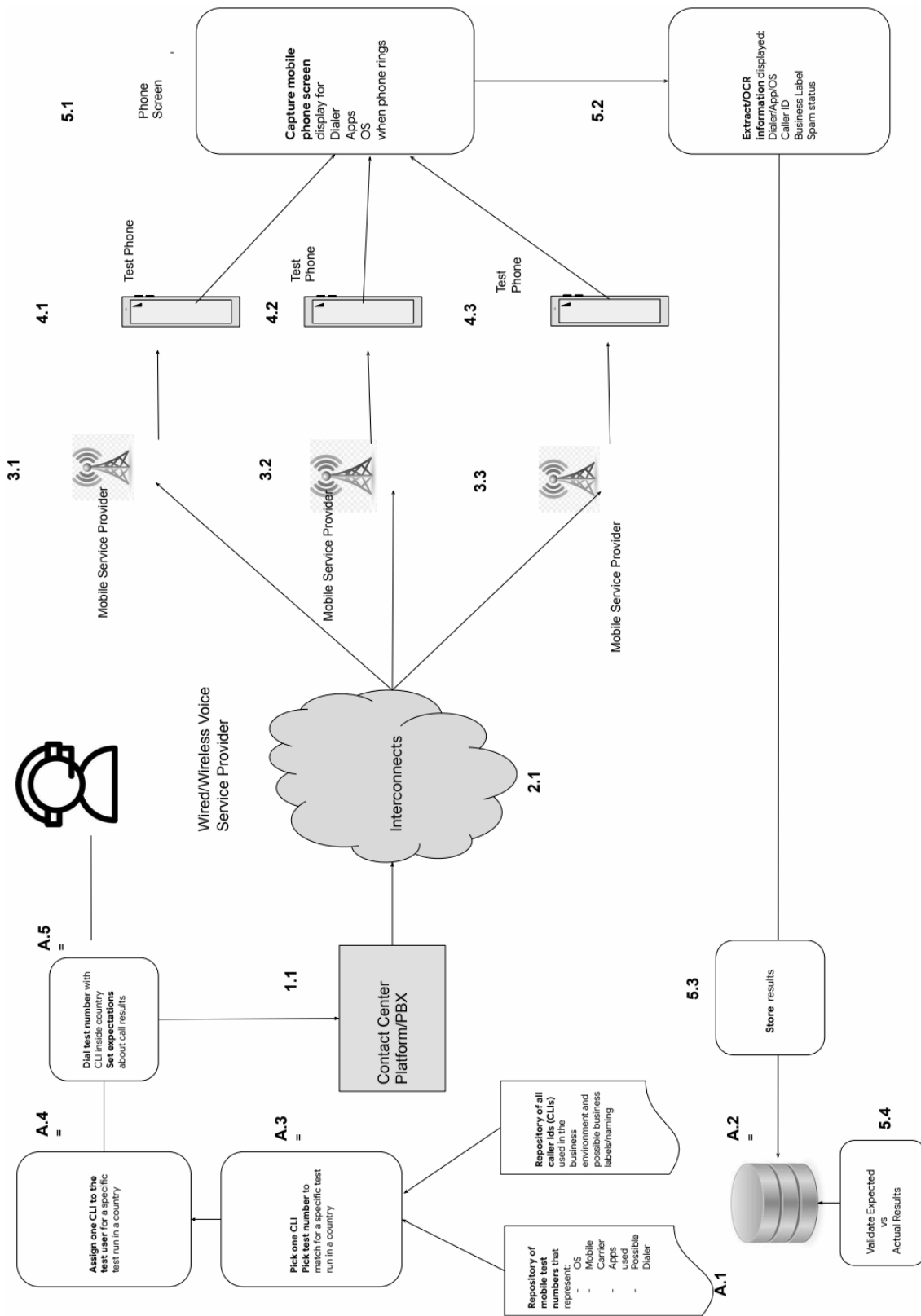


Fig. 1: Establishing phone number reputation using a contact center platform

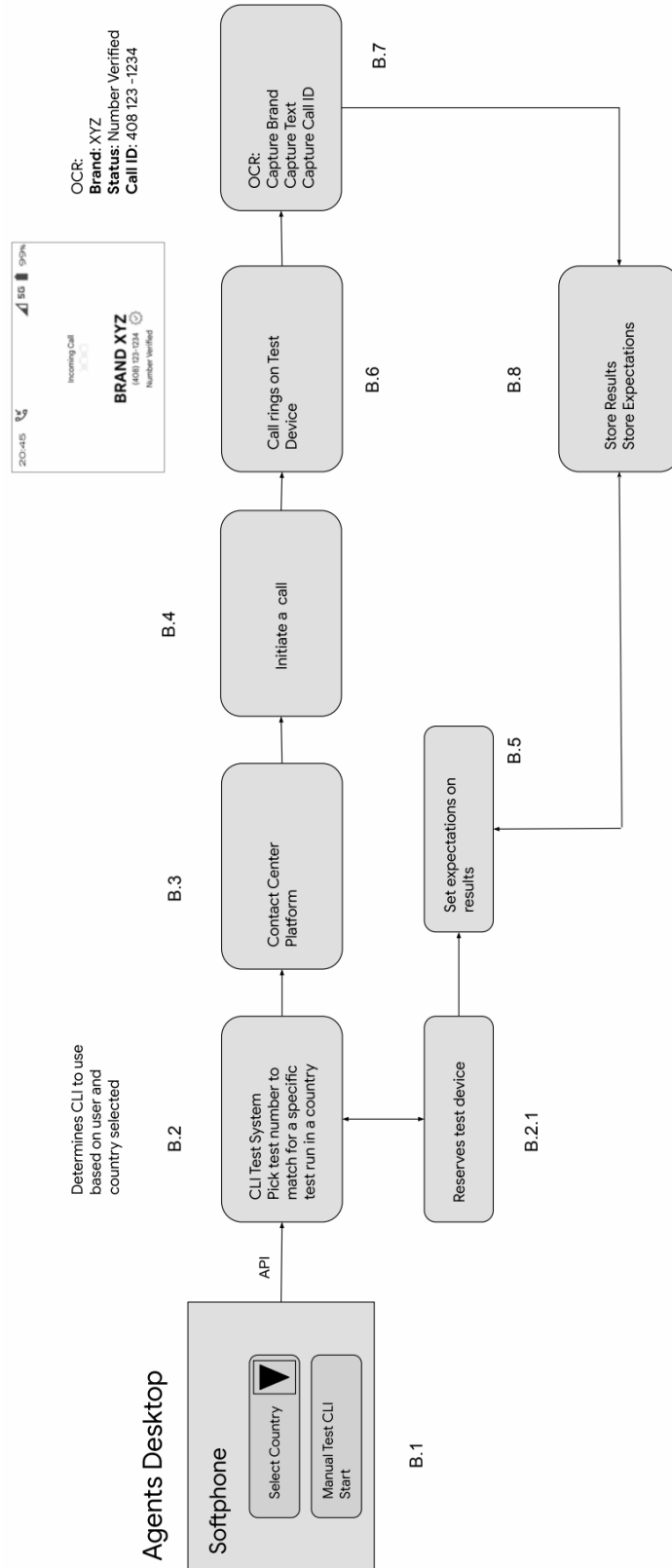


Fig. 2: Workflow for establishing phone number reputation using a contact center platform

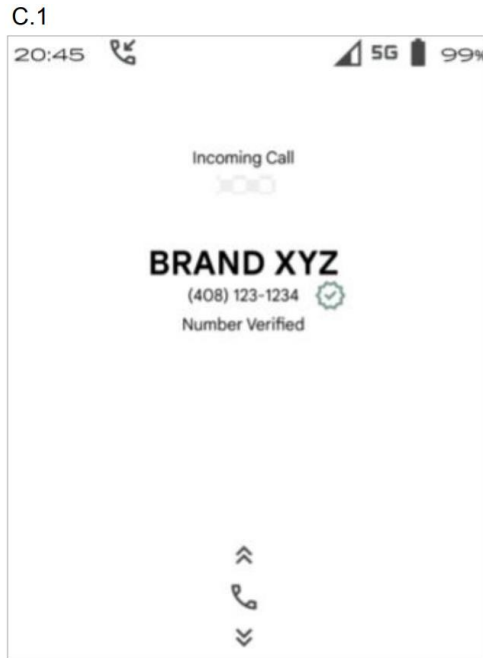


Fig. 3: An example screenshot taken automatically at a test mobile device upon the receipt of an incoming call

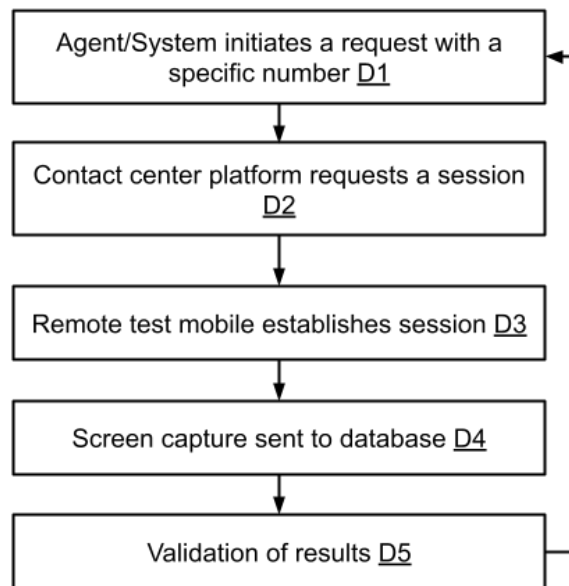


Fig. 4: Flowchart for validating caller ID results