WARWICK
THE UNIVERSITY OF WARWICK

14 May 2024

VIA ECFS

Marlene H. Dortch, Esq.
Secretary
Federal Communications Commission
45 L Street NE
Washington, DC 20554

Re: WC Docket No. 17-97 – Call Authentication Trust Anchor

Dear Ms Dortch,

First of all, we want to express our appreciation for the FCC’s relentless efforts in protecting phone users from scamming and caller ID spoofing attacks.

We represent a research team based at the University of Warwick in the UK. Our research focuses on investigating caller ID authentication solutions for heterogeneous telecommunication networks, funded by the Engineering and Physical Sciences Research Council (EP/T014784/1). We would like to submit an ex parte in response to the Commission's Notice of Inquiry (FCC 22-81), which seeks comments on caller ID authentication technologies for non-IP networks.

In the response below, we explain the major weaknesses of the STIR/SHAKEN system and present an alternative solution.

1. **STIR/SHAKEN authenticates carriers, not caller ID**

   The Notice of Inquiry describes STIR/SHAKEN as a “caller ID authentication” solution, technology or framework. We would like to highlight that in STIR/SHAKEN, authentication is done through digital signatures; only the carrier possesses the secret signing key, not the caller. Therefore, technically speaking, STIR/SHAKEN does not authenticate any caller ID; it authenticates the originating carrier where the call is made (or the gateway carrier for international calls that arrive inbound at the gateway). Strictly, STIR/SHAKEN is a “carrier authentication” solution.

   The distinction between “caller ID authentication” and “carrier authentication” is crucial as it explains the root cause of many reported cases of mislabelling, where a legitimate call is marked as a fraudulently spoofed one and vice versa. Even if we assume 100% adoption of STIR/SHAKEN across all networks, mislabelling will still be bound to happen because STIR/SHAKEN does not authenticate any caller ID per se.

2. **STIR/SHAKEN hands off the problem of caller ID authentication to carriers**

   While STIR/SHAKEN authenticates the carrier, the problem of authenticating the caller ID is left to carriers, and the process that they should follow to carry out this important task is undefined.

Carriers must include a label as part of the digital signature to attest (or claim) whether or not the caller is authorized to use the phone number. People sometimes modify their caller ID for legitimate reasons, e.g., using a phone at home to call customers but wanting them to call back a work number. The problem is that carriers don't always have the reliable information to distinguish between legitimate and illegitimate modifications of the number especially when the modified number belongs to a different provider. STIR/SHAKEN does not address this key problem.

The UK Ofcom public consultation in 2023 highlighted the need for STIR/SHAKEN to have "a common numbering database", available to telecom providers to determine whether the displayed call number is authentic or not. But creating and maintaining such a database was deemed infeasible and eventually Ofcom concluded that "we [the UK] should not proceed with CL authentication [STIR/SHAKEN] at this time"[1].

3. **Comment on "two standards for caller ID authentication on non-IP networks developed by the Alliance for Telecommunications Industry Solutions (ATIS)"**

We would like to clarify that neither standard performs "caller ID authentication". They authenticate the "carrier", not the "caller ID", hence addressing a different problem.

Authenticating the carrier in STIR/SHAKEN involves transmitting a digital signature along with a certificate chain in the payload, which can be several kilobytes. This is required for every call made. Non-IP networks were not designed to transmit such a large amount of digital data. Is the transmission of such a large amount of data really necessary since it only serves to authenticate the carrier, not the caller ID?

Our research shows that to authenticate the caller ID and to prevent illegitimate spoofing, it suffices to transmit only 4 digits, which can be well supported by existing networks (IP and non-IP). The choice of 4 digits limits the success rate for an illegitimate call-spoofing attempt to 0.01%. Consecutively failed spoofing attempts can be easily detected and blocked by the network. We explain more details below.

4. **Comment on "any alternative technological or policy solutions to enable caller ID authentication over non-IP networks"**

The alternative solution that we propose in the peer-reviewed paper published at *ACM Transactions on Privacy and Security* (2023) is called Caller ID Verification (CIV). Ofcom advises that when receiving a suspicious call with a genuine-looking number (e.g., the same number as shown on the bank account statements, in the phone book or on the company's or government department's website), users should hang up and call the number back to check whether the call was genuine.[2]

CIV follows a similar idea, however, it automates the otherwise manual call verification process based on a challenge-response protocol: upon receiving a call, the callee sends a short challenge (4 random digits) to the displayed number, and the caller needs to echo the same digits as a response to complete the caller ID authentication. This verification process is transparent to the caller and the callee.

[1] Ofcom consultation update (1 Feb 2024) https://www.ofcom.org.uk/__data/assets/pdf_file/0036/276687/01-24-cli-authentication-update.pdf

[2] https://www.ofcom.org.uk/phones-telecoms-and-internet/advice-for-consumers/scams/phone-spoof-scam

CIV does not require cross-border agreements for it to work effectively. For calls originating from overseas, we are primarily concerned with them spoofing a local number (neighbourhood spoofing) rather than another international number. When an incoming overseas call spoofs a local number, CIV sends a challenge to the local number and checks the response. Hence, deploying CIV domestically is sufficient to prevent spoofing calls from overseas or international gateways.

We have built proof-of-concept prototypes to show CIV works across different networks (landline, mobile and VoIP). Table 1 summarizes the differences between CIV and STIR/SHAKEN. We include more details about CIV in the appendix.

	STIR/SHAKEN	**CIV**
Authentication method	Digital signatures	Challenge-response
Authenticated subject	Carrier	Caller
Distinguishing legitimate and illegitimate spoofing	No (left to carriers)	Yes
Require a trusted governance infrastructure	Yes	No
Data transmission	Signature + certificate chain (several kilobytes)	4 digits
Telecom networks	IP only	Both IP and non-IP
Overhead	Certificates issuance, renewal, certificate revocation list (CRL) management, real-time validation of received certificates (likely involving round-trips to query external CRLs), etc	A round-trip to send and receive 4 digits

Last but not least, we want to thank you for your time and effort in coordinating the call for this Notice of Inquiry. We would like to propose an online meeting with the FCC and any interested stakeholders to explain our solution and answer any questions.

Yours sincerely,

Professor Feng Hao Department of CS University of Warwick, UK +44 24 765 72614 feng.hao@warwick.ac.uk WARWICK THE UNIVERSITY OF WARWICK	Basil Thomas Engineering Team Lead Squire Technologies +44 1305 757314 (ex 258) BThomas@squire-technologies.com squire technologies	Steve Smith Director trueCall Ltd +44 0208 408 8900 SteveSmith@truecall.co.uk trueCall™ STOPS NUISANCE CALLS

Appendix: an illustration of how CIV works in the telecom clouds

A peer-reviewed paper about the Caller ID Verification (CIV) protocol has been published in ACM Transactions on Privacy and Security (Vol. 27, No. 1, 2033). The paper's title is “Spoofing Against Spoofing: Toward Caller ID Verification in Heterogeneous Telecommunication Systems” (https://dl.acm.org/doi/10.1145/3625546). A freely accessible copy of the paper is available at: https://arxiv.org/abs/2306.06198.

In the paper, we have provided a proof of concept to show that CIV works across heterogeneous telecommunication systems (IP or non-IP networks) by modifying the software on the users’ phones. For practical deployments, we propose to implement CIV in the Telecom clouds instead of on the phones for optimal performance.

For simplicity, we assume both the originating and the terminating networks support CIV (we can also gracefully handle scenarios where only one of the networks supports CIV; see the paper for full details). The following illustrates how CIV works in three cases.

<u>Case 1: a legitimate caller uses the unmodified number</u>

In this case (most common), the callee’s carrier engages with the caller’s carrier in a challenge-response process to verify the displayed phone number. In our proof-of-concept implementation, we use number spoofing to embed the challenge (random four digits) in the last four digits of the caller ID of a verification call (Step 3) and use DTMF to send the response (Step 4). Other methods of sending the challenge and response are possible. Once the verification is successful, the caller ID (Alice’s number) is displayed on the receiver’s phone as shown in Figure 1.

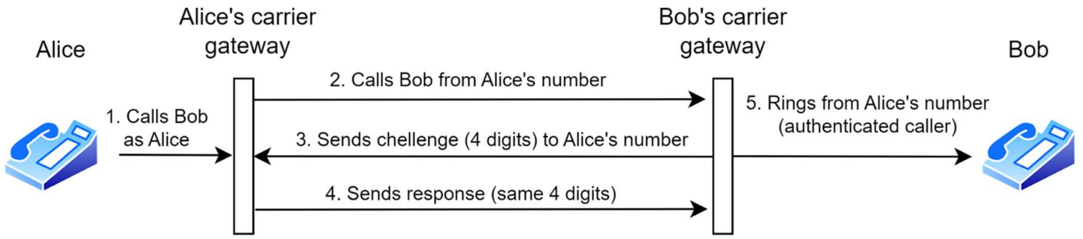
Alice
Alice's carrier gateway
Bob's carrier gateway
Bob
1. Calls Bob as Alice
2. Calls Bob from Alice's number
3. Sends chellenge (4 digits) to Alice's number
4. Sends response (same 4 digits)
5. Rings from Alice's number (authenticated caller)

Figure 1: authenticated caller ID with an unmodified number

<u>Case 2: a legitimate caller uses a modified number that they own</u>

In this case, the caller (Alice) modifies the caller ID to another number (Alice2) that she owns. Since Alice owns the other number, she can configure the call-forwarding function of that number, so that the challenge-response protocol still succeeds. The caller ID (Alice2’s number) is verified and displayed on the receiver’s phone as shown in Figure 2.

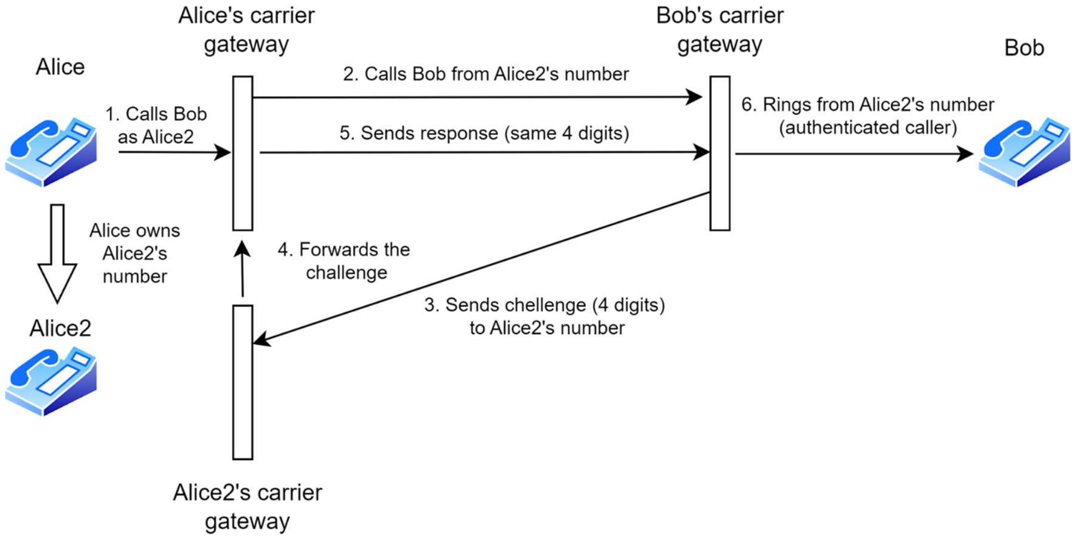
Alice's carrier gateway
Bob's carrier gateway
Alice
Bob
2. Calls Bob from Alice2's number
1. Calls Bob as Alice2
6. Rings from Alice2's number (authenticated caller)
5. Sends response (same 4 digits)
Alice owns Alice2's number
4. Forwards the challenge
3. Sends chellenge (4 digits) to Alice2's number
Alice2
Alice2's carrier gateway

Figure 2: authenticated caller ID with legitimate modification of the phone number

Case 3: an illegitimate caller uses a modified number that they don't own

In this case, the caller (Alice) modifies the number to one (Eve) that she doesn't own. When Eve's carrier receives the challenge, it finds that there is no matching record for Eve's outgoing call and there is no call-forwarding setting, hence it discards the challenge. Since Bob's carrier doesn't receive a correct response for the challenge, it concludes that the caller ID is unauthenticated, therefore rejecting the call. This is illustrated in Figure 3.

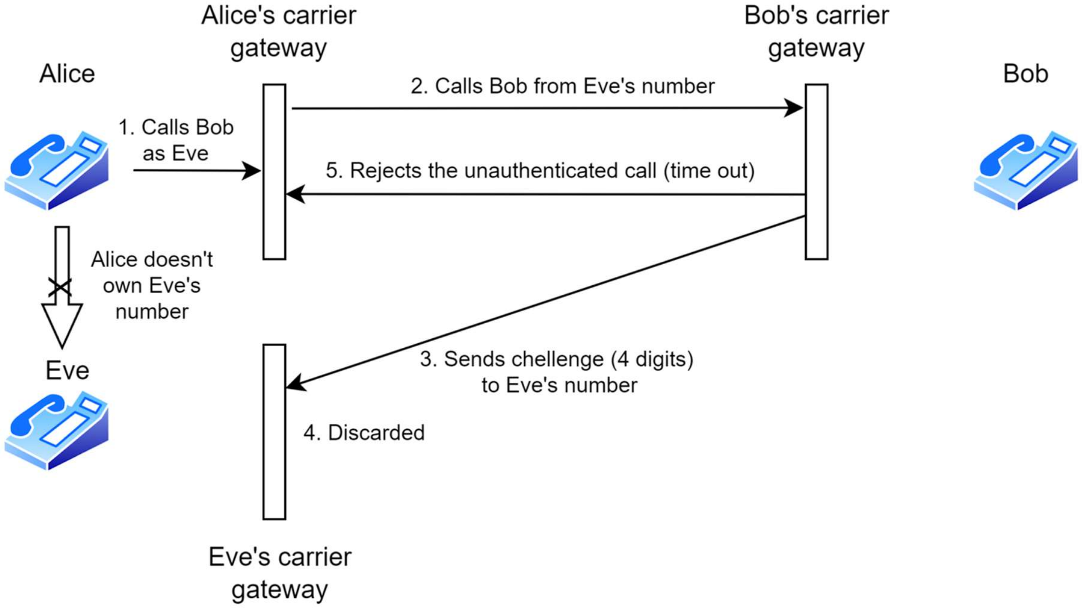
Alice's carrier gateway
Bob's carrier gateway
Alice
Bob
2. Calls Bob from Eve's number
1. Calls Bob as Eve
5. Rejects the unauthenticated call (time out)
Alice doesn't own Eve's number
3. Sends chellenge (4 digits) to Eve's number
Eve
4. Discarded
Eve's carrier gateway

Figure 3: unauthenticated caller ID with illegitimate modification of the phone number