Issues in Calling Line Identification (CLI) Authentication in the United Kingdom Based on the Experiences in North America

June 2021

Prepared for

Ofcom

by Richard D. Shockey
Shockey Consulting LLC

THE OPINIONS EXPRESSED ARE SOLELY THOSE OF THE AUTHOR AND DO NOT NECESSARILY REFLECT THE VIEWS OF OFCOM

CONTENTS

EXECUTIVE SUMMARY 1

METHODOLOGY USED IN THIS REPORT 2

1. A SIMPLE REVIEW OF CLI AUTHENTICATION BASED ON STIR/SHAKEN 3

2. THE EXPERIENCE WITH CLI AUTHENTICATION IN THE UNITED STATES 4

2.1. The Legal framework for STIR/SHAKEN CLI Authentication in the United States. 4
2.2. What is included in these Robocall Mitigation Plans? 6
2.3. Why were these technologies mandated in the US and Canada? 7
2.4. The governance structure for STIR/SHAKEN in the United States. 7
2.5. Funding the STIR/SHAKEN Infrastructure in the United States. 8
2.6. How successful has STIR/SHAKEN been in the US? 10
2.7. On the issue of Attestation – Full Attestation or nothing? 11
2.8. What happens if a call has no Attestation? 11

3. THE EXPERIENCE WITH CLI AUTHENTICATION IN CANADA 12

3.1. The framework for CRTC decisions on CLI Authentication. 13

4. THE STRUCTURE OF THE VOICE SERVICE NETWORKS IN THE UK 13

5. TECHNICAL ISSUES WITH THE DEPLOYMENT OF STIR/SHAKEN 14

5.1. Road Map Fatigue or “A Bridge Too Far”. 14
5.2. Canonicalization of the Telephone Number. 14
5.3. Packet Fragmentation or the TCP *versus* UDP Issue. 15
5.4. The Role of 608 and 607 SIP Error Codes. 15
5.5. Diversion or Call Forwarding. 15
5.6. The Framework of Certificate Revocation List Policy. 16
5.7. Know Your Customer. 16
5.8. Delegated Certificates. 16
5.9. Multihoming. 17
5.10. ALL Internet Protocol and SIP Interconnections are Fundamental to STIR. 17
5.11. Intercarrier Compensation Rules that Favour TDM Termination *versus* Internet Protocol.18
5.12. The Role of Data Analytics in CLI Authentication. 18
5.13. Legal Protection of the STIR/SHAKEN Data. 18
5.14. The Status of Out of Band (OOB) CLI Authentication Solutions. 19
5.15. Remediation in the event of a False Positive during the CLI Authentication. 20

6. FUTURE TECHNICAL DIRECTIONS IN STIR/SHAKEN BASED CLI AUTHENTICATION RICH CALL DATA TO DISPLAY 20

6.1. Issues with Call Branding and Registered Caller and other forms of Caller Registration. .22

7. THE ROLE OF STIR/SHAKEN IN TEXT MESSAGING 22

8. INTERNATIONAL COORDINATION WITH OTHER NATIONAL REGULATORY AUTHORITIES
23

9. RECOMMENDATIONS: OFCOM’S COURSE GOING FORWARD 23

9.1. Proceed with All Deliberate Speed. 24
9.2. STIR/SHAKEN is a Work in Progress. 24
9.3. Develop a National UK Numbering Database. 24
9.4. No Support for TDM/SS7 Networks. 25
9.5. Establish a Policy on Call Blocking. 25
9.6. Establish Guidelines on CLI Display. 25
9.7. Establish Traceback. 25
9.8. Continue to Work with NICC. 26

APPENDIX A: ABOUT THE AUTHOR 27

APPENDIX B: COMPANIES INTERVIEWED FOR THIS REPORT 29

EXECUTIVE SUMMARY

Readers of this report should understand that it is a snapshot of the current state of Calling Line Identification (CLI) Authentication in the United States and Canada. It should be understood that this process is in the early stages of deployment as of the first quarter of 2021 and there is substantially more to be done.

The United Kingdom (UK) continues to struggle with nuisance and, increasingly, scam calls. The ability to misuse Calling Line Identification (CLI) exacerbates this and impedes efforts to prevent or act against them. Major advancements in the technology of CLI Authentication have begun to be deployed in the United States and Canada.

The UK public should understand they are not alone. The Caller ID spoofing problem is a complex and multifaceted problem everywhere. No one single “silver bullet” is likely to magically solve the problem. In the United States and Canada, regulators and Service Providers have been taking aggressive action to mandate STIR/SHAKEN technology, in addition to other initiatives such as Traceback, to increase Enforcement efforts.

These efforts have generally been successful and hold great promise, but there is much work to be done, especially in the area of how CLI data and Verification parameters are displayed to consumers and enterprises.

Multiple protocol mandates in the United States are due by June 30, 2021, and in Canada by November 30, 2021. Additional mandates for call blocking notification are due in January 2022. Major United States and Canadian Operators have already made public statements that they have activated STIR/SHAKEN on their networks and are now exchanging CLI Authenticated traffic.

OFCOM, as the communications regulator of the UK, will have to undertake several steps in order to implement CLI Authentication. UK Voice Service Providers have already agreed to take an important first step towards these goals by planning to convert their networks to all Internet Protocol by 2025.

The first key step OFCOM should take is a general consultation among UK Service Providers to establish their commitment to implementing an appropriate governance framework for STIR/SHAKEN based CLI Authentication and fair and equitable funding mechanisms for these initiatives. The models for these governance authorities are well understood from the North American experience and should include all segments of the UK Voice and Messaging industry.

It is important for OFCOM and UK Service Providers to understand that STIR/SHAKEN based CLI Authentication will have to be a mandatory obligation on all UK Voice Service providers offering telephony services. This conclusion was among the most important issues the United States and Canadian operators and regulators decided upon. Either ALL providers comply with CLI Authentication, or the system will not work.

UK Voice Service providers have already deployed IP Interconnection agreements in some instances and should be able to substantially benefit from CLI Authentication until the full conversion of the UK networks to all Internet Protocol.

Second, OFCOM and the UK Service Providers should lay the groundwork for the implementation of National Centralized Numbering Databases (CDB) in the UK. These numbering databases will benefit UK Service providers in multiple ways, such as enabling the implementation of a more comprehensive Local Number Portability (LNP), Operator “Network Grooming” and translating the telephone number into an appropriate point of Internet Protocol interconnection. Such LNP platforms in the United States and Canada have been extremely successful in promoting competition among providers in all market sectors.

Third, OFCOM and UK Service providers should categorically reject proposals to implement CLI Authentication solutions specifically targeted at legacy Time Division Multiplexing and Signalling System 7 (TDM/SS7/C7) Class 4/5 networks. There is no evidence in the United States or Canada that these systems would work, and the protocols have not been properly approved. These efforts would be dangerously expensive, and essentially redundant given the commitment of UK operators to convert to all Internet Protocol by 2025.

METHODOLOGY USED IN THIS REPORT

The author of this report is intimately familiar with the technology and governance issues surrounding STIR/SHAKEN technology, and where the United States and Canadian Voice Service industry see future developments. I have undertaken multiple interviews with stakeholders in the United States, Canada and the United Kingdom to elicit their opinions. Many United States and Canadian operators have expressed a desire that their views be kept somewhat confidential. Consequently, views are generally aggregated without specific attribution to any one company or the national regulators of the United States and Canada. A list of companies and agencies interviewed is included as *Appendix B* to this report.

1. A SIMPLE REVIEW OF CLI AUTHENTICATION BASED ON STIR/SHAKEN

STIR/SHAKEN (Secure Telephony Identify Revisited/Signature-based Handling of Asserted information using toKENs) is a set of technical specifications developed by the Internet Engineering Task Force, the Alliance for Telecommunications Industry Solutions and the SIP Forum. These bodies have used these standards to address the robocall problem by creating a structure through which Originating Voice Providers attest (so far as they know) to the Caller Identity of their customers placing calls. STIR/SHAKEN then allows Terminating Voice Providers to validate the origin of the calling phone number, render an attestation of that call and potentially display that data to a consumer or enterprise in order for them to make an informed decision on whether to answer a call or not.

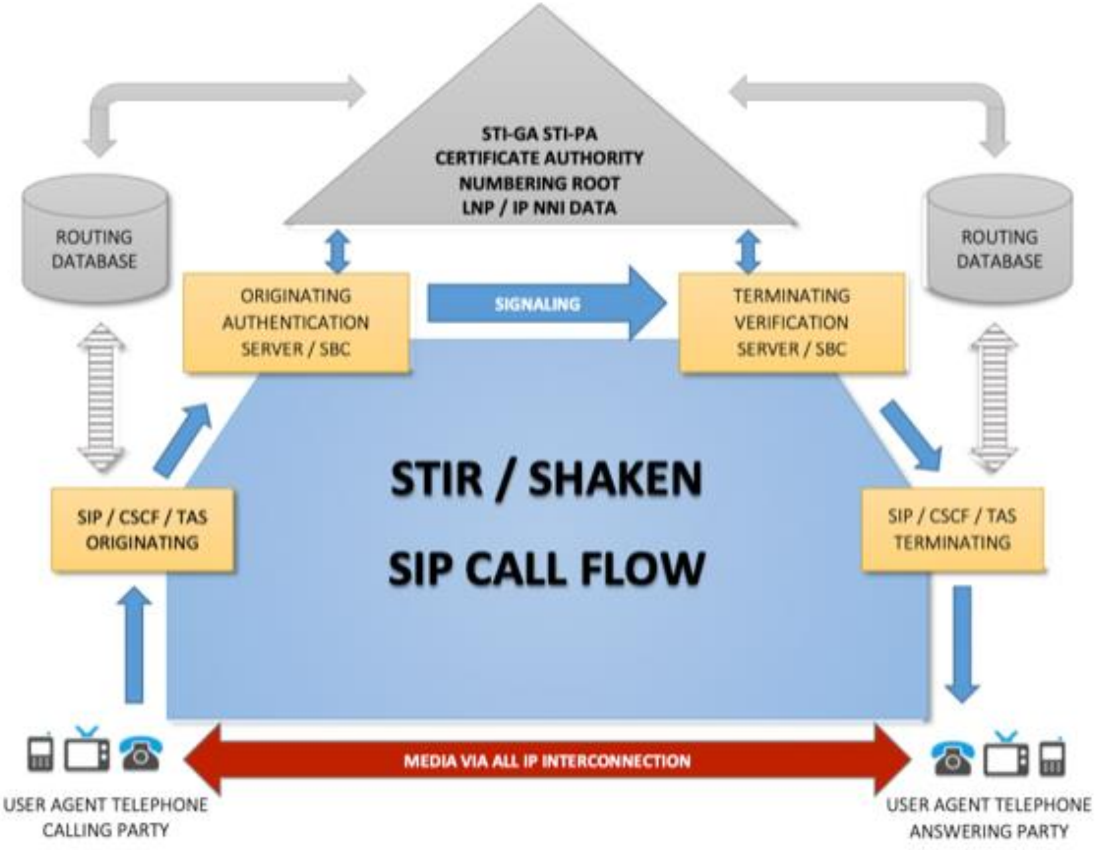
Robocalls, in the context of the United States and Canada, are typically defined as a telephone call from an automated source that delivers a prerecorded message to a large number of people. In many cases, such as public safety or a prior business relationship, these may be, in fact, legal and proper, but the term robocalls has come to mean any unwanted or nuisance call from a live or automated source that has an intent to defraud the consumer.

The STIR/SHAKEN system aims to add authenticated Public Key Infrastructure (PKI) to the SIP INVITE signalling headers that allow the points along the national Voice Service networks to positively identify the origin of the data. This does not directly prevent the ability for a robocaller to spoof a caller ID, but it does allow upstream points to decide whether or not to trust that ID. For STIR/SHAKEN to work, each carrier *must* hand-off SIP header tokens within the SIP INVITE to the next carrier in the call path. These SIP headers can *only* be passed over an Internet Protocol link. A traditional, time-division multiplexing (TDM) interconnection will not transmit a SIP header.

This author, in association with Scott Marcus of WIK Consulting, previously produced a report for OFCOM generally describing the underlying technology of STIR/SHAKEN and why certain decisions were made in its design.[1] All of those observations are as valid now as they were when that report was drafted.

The following diagram visualizes how the STIR/SHAKEN system is actually organized in United States and Canadian carrier networks.

[1] https://www.ofcom.org.uk/research-and-data/technology/telecoms/resource-public-key-infrastructure


STI-GA STI-PA
CERTIFICATE AUTHORITY
NUMBERING ROOT
LNP / IP NNI DATA
ROUTING DATABASE
ROUTING DATABASE
ORIGINATING AUTHENTICATION SERVER / SBC
SIGNALING
TERMINATING VERIFICATION SERVER / SBC
STIR / SHAKEN
SIP CALL FLOW
SIP / CSCF / TAS ORIGINATING
SIP / CSCF / TAS TERMINATING
MEDIA VIA ALL IP INTERCONNECTION
USER AGENT TELEPHONE CALLING PARTY
USER AGENT TELEPHONE ANSWERING PARTY

CSCF = Call Session Control Function | SBC = Session Border Control | TAS = Telephony Application Server

1. The SIP INVITE with the SIP Identity header, known as a PASSporT,[2] is sent by the originating service provider and received by the terminating service provider.

2. The terminating service provider invokes a STI Verification Service (STI-VS) to decode the SIP identity header and perform verification of the data transmitted in the call.

3. Depending on the results of the verification, information can be passed in a verification status or VERSTAT parameter in the SIP INVITE indicating the results of the verification step.

2. THE EXPERIENCE WITH CLI AUTHENTICATION IN THE UNITED STATES

2.1. The Legal framework for STIR/SHAKEN CLI Authentication in the United States.

The Authority to Act on CLI Authentication in the United States is very explicit and grounded in the TRACED Act of 2019 which passed the United States Congress by vast

[2] https://datatracker.ietf.org/doc/html/rfc8224

majorities and signed by the President of the United States.[3] This became United States Public Law No: 116-105. The Act empowers the United States Federal Communications Commission (FCC) to take affirmative action to implement STIR/SHAKEN as a mandate and report regularly to Congress on its progress.

The TRACED Act in the United States has been formally implemented by the FCC in two landmark orders known as the 2nd and 4th Report and Order.[4] [5] In addition, the FCC has presented to Congress a Report on its progress on CLI Authentication.[6]

The FCC has aggressively used its Authority to Act to change the very definition of what a Telecommunications Service Provider is. Under the current interpretation of a "Covered Entity", any operator that originates or terminates a voice call in the United States is now subject to FCC authority. This clearly includes such companies as Microsoft, Cisco, many popular collaboration platforms and third-party platforms such as Twilio, 5Nine and every intermediate transit provider that uses United States North American Numbering Plan numbers, irrespective of whether they were issued numbers by the North American Numbering Plan Administrator.

In addition, the FCC has mandated that all "Covered Entities" are required to file a Robocall Mitigation program with the FCC by June 30, 2021. The penalty for noncompliance is a prohibition on any form of voice interconnection. This may be viewed as the "Nuclear Option" or "Excommunication" as it would prevent any Covered Entity in connecting any ingoing or outgoing traffic.

> "We additionally create a certification process and database to aid in enforcement efforts and prohibit intermediate providers and terminating voice service providers from accepting voice traffic from voice service providers not listed in the database. These steps will ensure that the only voice traffic to traverse voice networks in the U.S. is from those voice service providers that have either fully implemented STIR/SHAKEN on their entire networks or that have implemented a robocall mitigation program on those portions of their networks that are not STIR/SHAKEN-enabled."

Recently the FCC has invoked this option for several carriers.[7]

[3] https://www.congress.gov/bill/116th-congress/senate-bill/151/text

[4] https://docs.fcc.gov/public/attachments/FCC-20-136A1.pdf

[5] https://docs.fcc.gov/public/attachments/FCC-20-187A1.pdf

[6] https://www.fcc.gov/document/report-congress-caller-id-authentication-implementation-process

[7] https://www.fcc.gov/document/acting-chairwoman-rosenworcel-kicks-anti-robocall-agenda

2.2. What is included in these Robocall Mitigation Plans?

The FCC has provided some guidance on what these plans should look like, but in general, Service Providers MUST provide information that addresses several issues.[8]

1. Document what steps the service provider is taking to avoid originating illegal robocall traffic.
2. Support STIR/SHAKEN in the IP portions of their networks.
3. The Service Provider must commit to respond to requests from the Traceback Consortium to trace suspect calls.
4. Take proactive steps to “know your customer” and understand where its voice traffic is coming from. [9] [10] [11] [12]

The Federal Trade Commission is also actively involved in these efforts, principally through enforcement actions.[13] Of particular note, the Attorney Generals of all fifty United States and numerous carriers have agreed on a set of principles to combat robocalls and urged Industry to further accelerate its efforts.[14]

Part of the TRACED act was a mandate for the establishment of a Traceback Consortium that would assist Law Enforcement, the FCC and the United States Federal Trade Commission and State Attorney Generals in tracking down the origin of robocalls.[15] Voice providers are now required by FCC Order to respond to any request from the Traceback Consortium on demand.[16]

Traceback is much easier in an all Internet Protocol environment versus a classic TDM/SS7, since the SIP INVITE contains vastly more information about the origin of the call than a classic Call Detail Record.

[8] https://www.fcc.gov/document/fcc-issues-caller-id-authentication-best-practices

[9] https://commlawgroup.com/2021/now-that-the-robocall-mitigation-database-is-available-your-company-needs-a-robocall-mitigation-plan-stat-what-is-it-and-how-the-commlaw-group-can-help

[10] https://www.kelleydrye.com/KelleyDrye/media/News-Pubs-and-Events-Images/KelleyDrye-Robocall-Mitigation-Plan-Checklist.pdf

[11] https://www.dwt.com/insights/2020/10/fcc-stir-shaken-robocall-mitigation-plan-deadline

[12] https://www.jdsupra.com/legalnews/multiple-new-fcc-robocall-initiatives-9820905

[13] https://www.consumer.ftc.gov/articles/0259-robocalls

[14] https://www.natlawreview.com/article/state-attorneys-general-and-voice-service-providers-agree-anti-robocall-principles

[15] https://www.ustelecom.org/the-industry-traceback-group-itg/

[16] https://docs.fcc.gov/public/attachments/FCC-20-187A1.pdf

2.3. Why were these technologies mandated in the US and Canada?

It has been the consensus of participants in the TRACED Act process, including major United States Voice service providers, that a mandate to implement STIR/SHAKEN and Traceback was necessary in order to ensure universal compliance. There was some concern that if only major Voice Service Providers were in compliance, smaller providers would hesitate or refuse to take proactive action citing cost issues or lack of technical expertise. On that basis the argument was, unless EVERYONE does this, it would not work.

This argument has been consistently used in the legal framework for United States and Canadian telecommunications regulation. The last time this argument was used was in the debate over the 1996 US Telecom Act, specifically over the issue to Local Number Portability. Local Number Portability (LNP) became one of the most important pro-completion provisions of the United States 1996 Communications Act. LNP works and the use of Centralized Numbering Databases made that possible, though at considerable expense to Operators.

2.4. The governance structure for STIR/SHAKEN in the United States.

Shortly after the passage of the TRACED Act, various United States Voice Service providers self-organized into an industry “co-regulatory” body to address CLI Authentication governance. It is known as the Secure Telephone Identify Governance Authority (STI-GA). The Alliance for Telecommunications Industry Solutions was selected as a Secretariat. Careful attention was paid to having a diverse set of stakeholders act as a Board of Directors.[17] The STI-GA designed a Secure Telephone Identity Policy Authority (STI-PA) to administer the distribution of X.509 Cryptographic material among all authorized United States Voice providers.[18] All United States Voice Service Providers that use United States North American Numbering Plan (NANP) numbers *must* obtain authorized X.509 Certificates in order to participate in the STIR/SHAKEN system. There is considerable discussion in the United States STI-GA about expanding the entities that can obtain Certificates and some conclusions have been made to include non-traditional, non-facilities-based Voice Service providers.

The United States Federal Communications Commission, though not involved directly in the STI-GA or STI-PA operations, has clearly stated it will retain overall plenary authority and oversight of these institutions as authorized by the TRACED Act and under its authority over telephone numbering defined under 47 USC § 251 (e) 1.

[17] https://sti-ga.atis.org/

[18] https://authenticate.iconectiv.com

The Federal Communications Commission has often used the North American Numbering Council (NANC) to draft policy recommendations.[19] The NANC operates as a formal United States Federal Advisory Committee within and under the auspices of the FCC. The author of this report sits on that Committee.

The NANC Call Authentication Trust Anchor (CATA) working group provided the FCC with multiple reports and recommendations on how to implement CLI Authentication in the United States.

During the STIR/SHAKEN process, each service provider will create a SIP identity header at Call Origination. This header contains the following information about the incoming call:

- Calling number
- Called number
- Timestamp
- Attestation level
- Origination identifier
- Location
- Digital signature

There has been discussion in the United States about ensuring that these headers are fully protected from being tampered with or deleted by using regulatory language similar to that contained in the United States Code of Federal Regulations that protects billing data.[20]

2.5. Funding the STIR/SHAKEN Infrastructure in the United States.

The FCC and the Voice Service industry in the United States have often organized Quasi Non-Governmental Organizations (QUANGOs) for managing various industry numbering resources.

For example, the United States Local Number Portability database administration is principally organized by a QUANGO through the NAPM LLC,[21] as well as funding for telephone number allocation,[22] the Telephone Number Pooling Administration and a newly created Reassigned Number Database.

[19] http://nanc-chair.org/

[20] https://www.law.cornell.edu/cfr/text/47/64.1601

[21] https://napmllc.org/

[22] https://www.nationalnanpa.com/

The goal in all these instances is a fair and equitable distribution of costs associated with these databases from all participants in the process.

The United States and Canada use multiple models to achieve these objectives. The cost recovery model for how the UK STIR/SHAKEN administration or Secretariat for these functions needs to be selected.

In the case of the United States STI-GA, initially the Board of Directors “passed the hat” among Voice Service providers in order to recover various costs associated with start-up costs based on a three-year budget. On the basis of that funding, the STI-GA began the process of an open tender process for the operation of the STI-PA.

The North American Portability Management LLC selected a membership model for its administrative and legal costs.

The North American Numbering Plan Administration (NANPA) is directly controlled by, and the contract for operation is shared by, the regulatory authorities of the thirteen nation states that comprise E.164 Country Code +1.

The actual funding mechanism for the day-to-day operations of these functions takes two forms:

(1) Funding for these network functions among providers is generally accomplished by a mechanism generally referred to as Cost Allocation. The principal method of cost allocation for Number Administration is to make an assessment of the appropriate contribution to the total WORKING telephone numbers each entity has in the network. Both the United States and Canada have annual forms that must be filled out indicating the actual working numbers, as well as numbers that have been allocated, but held in inventory, for new customers. In the United States this is known as the Number Resource Utilization and Forecast (NRUF).[23] In addition, numbers can be recovered from service providers at the direction of the NANPA administrator and reallocated to other providers. Once a budget is developed and approved, with the full knowledge and consent of the regulator, the reported data is used to develop an Allocation Model and a Contribution Factor is developed. A simple calculation can then be made and prepared for billing.

(2) In the case of the US Number Portability Administration Centre (NPAC), the allocation model is based on a percentage of revenue of the telecom providers. All Eligible

[23] https://www.nationalnanpa.com/nruf/

Telecommunications Carriers are required to file FCC Form 499-A with the FCC that lists their telecom revenue.[24]

The United States STI-GA has recently selected a Cost Allocation model based on Industry revenue.[25]

In contrast, Canada combines the Cost Allocation model with what is known as the Cost Causer model for Canadian Local Number Portability functions. In that scenario, it is the entity that triggers the number port that must pay the determined rate for that function. This is also true for what is known as mass Network Grooming operations.

The United States does not use a Cost Causer model for any number of historical reasons. It has chosen to negotiate an annual fixed price for LNP functions, and the Allocation Model is run based on the contract negotiated with the vendor of the database.

Billing functions can be handled by a third-party accounting firm, as in the case of the NANPA, or can be billed directly by the regulator.

All of these methods are widely supported by United States and Canadian Voice Service providers.

2.6. How successful has STIR/SHAKEN been in the US?

As of the date of this report it is somewhat difficult to determine the actual status or success of CLI Authentication deployments. Deployments are in early stages and there have been significant technical barriers to adoption. That said, there has been considerable success among several sectors of the United States Service providers. Nearly 90% of all voice calls that originate and terminate between providers of Mobile Access networks are now compliant: this includes ATT, Verizon and T-Mobile. The reason for this is that they have been all Internet Protocol SIP/IMS for some time and interconnect via Internet Protocol as well. This is also true for the major Cable Operators that have large scale Fiber/CoAxial Access Networks. Comcast, Cox Communications and Charter Communications were early adopters of SIP/IMS and have interconnected their traffic using Internet Protocol for many years. Internet Protocol Voice Peering agreements have been in place among many of these providers for some time.[26] [27]

[24] https://numberportability.com/resources/faq/

[25] https://sti-ga.atis.org/wp-content/uploads/sites/14/2020/11/201118-STIGA-Board-Policy.pdf

[26] https://www.t-mobile.com/news/network/stir-shaken-all-networks

[27] https://www.fiercewireless.com/operators/verizon-starts-verifying-calls-other-carriers-using-stir-shaken

2.7. On the issue of Attestation – Full Attestation or nothing?

It is useful to review what the STIR/SHAKEN framework says about Call Attestation passed from the Originating Network to the Terminating Network.

Currently there are 3 levels of Attestation:

A. Full Attestation. The signing provider:

- is responsible for the origination of the call onto the Internet Protocol based service provider voice network;
- has a direct authenticated relationship with the customer and can identify the customer; and
- has established a verified association with the telephone number used for the call.

In essence Carrier A says to Carrier B: “This is my customer. I gave him this telephone number. This call originated on my network. You can trust it.”

B. Partial Attestation. The signing provider:

- is responsible for the origination of the call onto the telephone network;
- has a direct authenticated relationship with the customer and can identify the customer; and
- has NOT established a verified association with the telephone number being used for the call.

C. Gateway Attestation. The signing provider:

- is the entry point of the call onto the telephone network; and
- has no relationship to the initiator of the call (*e.g.,* international gateways).

Multiple commentators to this report have indicated that they will support only Full Attestation. It is not clear whether service providers have any interest in Partial or Gateway Attestation even for International Call Gateways. The reasons of this are unclear. The FCC and the Canadian Radio-Television Communications (CRTC) have not required the use of Partial or Gateway Attestation at this time. This author and others have suggested the Attestation Model could/should be more granular to cover more use cases, but such suggestions have been rejected by the relevant Standards Development Organizations.

2.8. What happens if a call has no Attestation?

Whether there has been a fault in the CLI Authentication framework or the call is from a legacy TDM network, the default network behavior is simply to let the call go through unless the call meets various criterion for automatic Call Blocking. Information on Non-Authentication, for the time being, is not given to the called party.

3. THE EXPERIENCE WITH CLI AUTHENTICATION IN CANADA

The Authority to Act by the CRTC is defined in its Enforcement Decision 2019-404.[28] Under this Order, compliance with the STIR/SHAKEN mandate is defined as a condition of offering and provider of telecommunications services as defined by Canadian Telecommunications Law.

The Canadian Interconnection Steering Committee (CISC), a technical advisory body to the Canadian Radio-Television Commission (CRTC), has undertaken the principal role of advising on various aspects of how STIR/SHAKEN is being implemented in Canada.[29] [30] In general, the process has gone very smoothly with Canadian Operators seeing virtually the same technical issues as their United States counterparts.

It is the judgement of this author that Canadian Operators and regulators are operating in virtual lock step with their United States counterparts and will continue to follow broadly the same path.

Canadian Operators are also required to submit a STIR/SHAKEN Implementation Readiness Assessment to the CRTC by August 31, 2021, in accordance with their STIR/SHAKEN Implementation Order 2021-123 issued by the Compliance and Enforcement Division of the CRTC.[31]

Commentators have noted some difficulty with negotiating Fair, Reasonable, and Non-Discriminatory (FRAND) all Internet Protocol Interconnection Agreements with some Incumbent Operators, knowing that lack of Internet Protocol interconnection between providers could defeat the purpose of CLI Authentication. This, again, matches the experience of some in the United States.

[28] https://crtc.gc.ca/eng/archive/2019/2019-404.htm

[29] https://crtc.gc.ca/eng/cisc-cdci.htm

[30] https://crtc.gc.ca/cisc/eng/cisf3d0b.htm

[31] https://crtc.gc.ca/eng/archive/2021/2021-123.htm

3.1. The framework for CRTC decisions on CLI Authentication.

Recently the CISC presented the CRTC with Status Report Framework for STIR/SHAKEN in Canada (NTWG TIF 40).[32]

This report represents a very concise and responsible snapshot of the status of CLI Authentication in Canada. The report concludes that TDM/SS7 networks are obsolete, an observation that both OFCOM and UK operators have also noted. This report also concluded that various Out of Band solutions for legacy networks have not been published by the relevant standards bodies and will not be used in Canadian Networks in the short term, if ever.

The Canadian CISC report also notes various technical issues that are literally identical to those the FCC and United States operators face.

The role of the STI-GA in Canada has been undertaken under the administrative umbrella of the Canadian Local Number Portability Consortium.[33] This was, in the author’s opinion, a wise, cost effective and prudent decision to use existing structures.

4. THE STRUCTURE OF THE VOICE SERVICE NETWORKS IN THE UK

It is clear that large portions of the UK Voice network could implement STIR/SHAKEN CLI Authentication in the near term.

The majority of Voice Traffic in the UK is now originated or terminated on the Mobile networks. Estimates are that 70% of voice is mobile, which parallels the situation in the United States and Canada. Though many of those networks still use legacy 3G networks, they are rapidly being upgraded to 4G and 5G, using Voice Over LTE (VOLTE) based on SIP rather than legacy “circuit switched” TDM voice. Consequently, most of mobile-to-mobile voice traffic will be SIP based on an end-to-end basis in the near term.

A significant proportion of fixed voice calls are also originated or terminated on Internet Protocol networks. Moreover, fixed operators are expected to retire the remaining TDM networks over the next five years. The author therefore believes that STIR/SHAKEN could be implemented here in the very near term on the basis that the transition to Internet Protocol will be completed in just a few years. There are initiatives to retrofit support for STIR/SHAKEN to

[32] https://crtc.gc.ca/cisc/eng/cisf3d0g.htm

[33] https://clnpc.ca/

TDM C7 signalling but the accepted wisdom is that this is disproportionate given that TDM networks will soon be retired.

Though UK Voice Service networks do not currently deploy centralized numbering databases for applications like Local Number Portability, this should not preclude early adoption by those operators that are currently Internet Protocol ready or will be in the short term.

5. TECHNICAL ISSUES WITH THE DEPLOYMENT OF STIR/SHAKEN

Those interviewed for this report have identified a number of technical issues related to STIR/SHAKEN deployment. Most of the issues are generally “teething pains” from the introduction of new technology into the network. This is to be expected as STIR is a complex technology. OFCOM and UK Operators need to understand what they will be facing. United States and Canadian operators have already faced these problems with the introduction of LNP in the early 2000s and SIP/IMS into the core over the last fifteen years. Operators have emphasized that these enhancements cannot be rushed into the network but require considerable laboratory testing before field deployment. New software can often result in incompatibilities further into the network itself.

5.1. Road Map Fatigue or “A Bridge Too Far”.

Many United States and Canadian contributors to this report have indicated that their organizations have exhibited symptoms of a malady known as “Road Map Fatigue”. In this scenario, multiple and shifting regulatory requirements that are driving network upgrades produce a level of exhaustion in Network Engineering Staff, as well as Chief Financial Officers. Interoperable National Voice networks are inherently complicated systems and deployment of these new requirements cannot be rushed.

5.2. Canonicalization of the Telephone Number.

Not all network elements perform canonicalization consistently – this can result in improperly signed calls that do not get verified correctly. Both the SIP FROM: and TO: in the SIP INVITE should be in the fully expressed E.164 format as in [+ 44 (number)]. It is the FROM: number that is used to cryptographically sign the signalling.

Some enterprises or networks still do not send calls to the Originating Network in proper E.164 format, leaving the burden of trying to “normalize” the Calling Party numbers on the network element signing or verification request. This can easily result in a failed verification at the Terminating party network.

5.3. Packet Fragmentation or the TCP *versus* UDP Issue.

Many carriers still use UDP, rather than TCP, for SIP signalling. The increasingly large SIP INVITE containing the Identity header may be fragmented, so the carriers' Internet Protocol Transport networks must be capable of handling fragmentation and re-assembly of SIP INVITE packets to ensure intact delivery of the Identity header. In addition, Provider edge network elements, such as Session Border Controllers, have not universally enabled TCP Keep Alive, resulting in dropped calls.

5.4. The Role of 608 and 607 SIP Error Codes.

The 4th Report and Order on Robocalls from the FCC mandated the implementation of the IETF RFC 8688 and the issuance of a 608 (calls rejected by an intermediary party that is not the recipient) or 607 (calls unwanted by the recipient) SIP error code in the event a call was blocked by the terminating Voice Service provider.[34] This was at the explicit request of many call originators who have bitterly complained about Call Blockage from legitimate providers.[35] Many commentators have noted that vendors have not implemented IETF RFC 8688 in their products, have no roadmap on when it will be implemented and that implementation within the time frame of the FCC 4th Report and Order January 2022 is, perhaps, unrealistic.[36] The resolution of this issue is unclear.[37]

Commentators have noted that Call Blockage is considered almost automatic in certain cases, such as a regulatory prohibition on accepting calls that have malformed national numbers, numbers that have not been issued to service providers, numbers that are deemed exceptionally prohibited (Do not Originate), such as numbers issued to Public Safety Institutions or numbers that have been discontinued but not reassigned.

5.5. Diversion or Call Forwarding.

As an example, Carrier A's network sends a call with Identity header to User B in Carrier B's network. However, User B has his device forwarded to User C in Carrier C's network, and Carrier B passes the original Identity along. This Identity will fail verification in Carrier C's network because Carrier C will assume User C is the destination number, whereas the Identity

[34] https://datatracker.ietf.org/doc/rfc8688/

[35] https://ecfsapi.fcc.gov/file/10501047411526/ABA_Comment_Letter_Call_Blocking_Second_Staff_Report_2021_04_30_final.pdf

[36] https://ecfsapi.fcc.gov/file/10506243707563/USTelecom%20-%20Notification%20PFR-Request%20for%20Clarification%20050621%20-%20FINAL.pdf

[37] https://www.neca.org/docs/default-source/wwpdf/public/6421adhoc.pdf

has User B as the called number. How this is going to work going forward is still under discussion in various technical forums.

5.6. The Framework of Certificate Revocation List Policy.

Concurrent with the policy issue of what entity gets a STIR/SHAKEN Certificate token, under what circumstances would that Certificate be revoked and who orders the Revocation? This is fundamentally a policy issue that will be jointly undertaken by the United States STI-GA and the FCC and needs to be considered as part of establishing any STIR governance model.

5.7. Know Your Customer.

This concept relates to the demands of the TRACED Act that Wholesale Providers of Voice Services should actually know who their customers are and police their activities, since it is clear that a significant percentage of robocall traffic is generated through this marketplace and often outside United States, UK and Canadian borders. This is critically relevant since the failure to comply or participate in FCC mandated Traceback activities could result in a denial of interconnection.

5.8. Delegated Certificates.

This is one of the most contentious issues in STIR/SHAKEN deployment. Many Voice Service providers, specifically those that provide services to Contact Centers or Enterprises, may not fit the profile for obtaining STIR/SHAKEN credentials directly, but want a measure of control in how their calls are signed. Some Enterprises are concerned they will not be able to sign their own calls, should they desire to do so.

Delegated Certificates may address this problem, but the solution is complicated to implement. A Delegated Certificate is one that has been derived from the Originating Service provider to another entity that wishes to sign their own calls. This would be a Delegation of Authority from the Service Provider that obtained numbers from the Regulator to an Enterprise that makes a significant amount of outbound calling, such as the Financial Services industry, Health Care or even Government.

As in many aspects of STIR/SHAKEN this is a work in progress.[38] [39]

[38] https://access.atis.org/apps/group_public/download.php/47134/IPNNI-2019-00043R000.pdf

[39] https://www.bandwidth.com/blog/stir-shaken-101-do-you-need-to-sign-your-own-calls/

5.9. Multihoming.

Many Enterprises and Call Centers use more than one Service Provider to terminate calls, even if the telephone number has been issued by another provider. The business case for this is to ensure that the Enterprise or Call Center is not dependent on one carrier for call completion, in the case of a carrier network failure, or to negotiate better pricing for voice services. Multihoming is, in part, related to the delegated certificate issue in that if Entity A has signed a call but uses Carrier A and Carrier B for competitive reasons and then how are those credentials going to be treated by the networks. This issue has not been fully resolved.

There is some evidence that some service providers are starting to negotiate bi-lateral agreements between the Enterprise or Call Center and the Service Provider that if the Service Provider sees traffic from certain trunk groups, it will be given an attestation, irrespective of whether the number came from Carrier A, B or C. The Enterprise or Entity itself would have to attest to their right of use for those numbers. This could solve the multihoming problem. However, there is no policy decision yet on whether this is acceptable.

5.10. ALL Internet Protocol and SIP Interconnections are Fundamental to STIR.

In the United States and Canada this is a major issue. As UK Voice Service operators are working to a broadly agreed timetable on the sunset of the UK TDM/SS7/C7 networks by 2025, United States and Canadian operators are not. The author’s own estimates to the FCC have indicated perhaps 35% of all US calls will not be validated unless the FCC sets a Sunset Date.[40] In addition, multiple commentators have reported serious issues with negotiations over all Internet Protocol Interconnection Agreements. In the United States and Canada these are considered unregulated agreements bi-laterally agreed to under terms and conditions that are opaque to both regulators and other operators. In some cases, commentators have reported that incumbent carriers have refused to negotiate fair, reasonable and equitable agreements for Internet Protocol interconnection under any conditions. Commentators have noted that this might put them at a competitive disadvantage, since even though a call could be properly signed by a competitive carrier at Origination, if an incumbent refuses to Internet Protocol Interconnect via SIP to terminate the call, the CLI Authentication will be lost if it had to be routed to TDM/SS7.

[40] https://ecfsapi.fcc.gov/file/1030722789616/Shockey%20Consulting%20FCC%20Exparte%20WC%2017-97%20March%202021%20copy.pdf

5.11. Intercarrier Compensation Rules that Favour TDM Termination *versus* Internet Protocol.

There is ample evidence from multiple commentators that the current United States Intercarrier Compensation rules favor TDM termination over Internet Protocol termination, even if an Internet Protocol interconnection agreement is actually in place. The reason for this is money. Section 201-251 of the United States Telecommunications Act still allow for Compensation under Originating Access rules. Though the amounts of money involved are somewhat small, they represent a barrier to CLI Authentication adoption that both the FCC and CRTC in Canada (where similar issues arise) will need to address.

5.12. The Role of Data Analytics in CLI Authentication.

The Canadian CISC report has indicated that they have not sufficiently investigated the role of Data Analytics in the Call path. Commentators from the UK have made similar observations. In the United States, this issue is already well understood. All United States major Voice Service providers, including all the major Mobile Access operators, now deploy Data Analytics. Call Authentication Data Analytics is roughly defined as a network element at the originating network that looks at the origin of the call and performs a variety of tests against that number using various forms of Artificial Intelligence, database look ups, historical data, etc. to determine if the call should be blocked or how it may be treated and what, if any signalling to the consumer may be appropriate. In the United States. these services are principally performed by four providers: Hiya,[41] TNSI,[42] First Orion,[43] and NeuStar[44], though other solutions are also offered.

5.13. Legal Protection of the STIR/SHAKEN Data.

One of the issues OFCOM should consider is the protection of CLI Authentication data within the UK Voice Networks. In the United States, data protection of call signalling data has been enshrined in the US Code of Federal Regulations.[45] These Regulations are designed to protect signalling data across the network that protect billing data necessary to permit the call to be charged or accounted for in Intercarrier Compensation.

[41] https://www.hiya.com/

[42] https://tnsi.com/

[43] https://firstorion.com/

[44] https://www.home.neustar/

[45] https://www.law.cornell.edu/cfr/text/47/64.1601

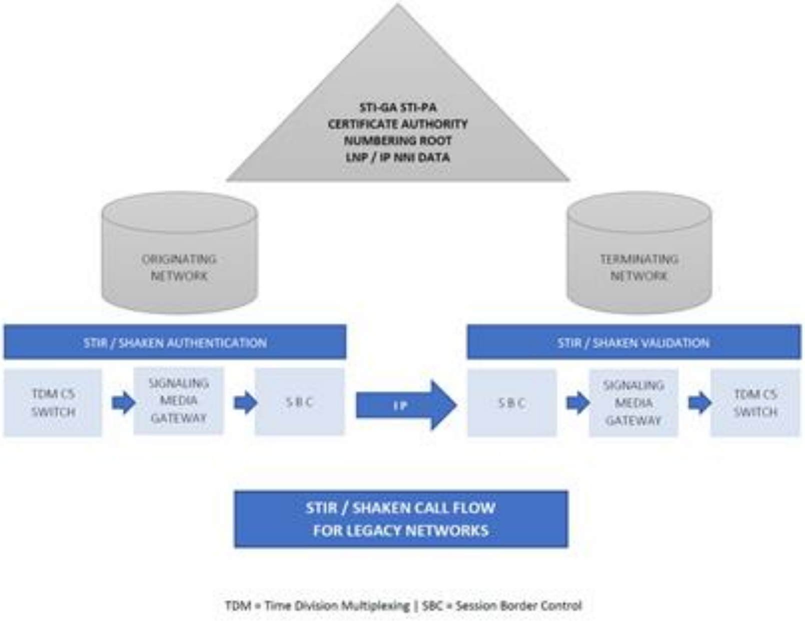
5.14. The Status of Out of Band (OOB) CLI Authentication Solutions.

There has been much discussion of how CLI Authentication might be implemented in legacy TDM Networks. Several technical initiatives in the IETF have looked into this problem.[46] As of the date of this report, those draft standards have not been approved.

It is the strong opinion of the author that the proposed standard in the IETF should be ignored by UK operators and regulators.

Multiple commentators that the author has spoken with are adamant that the solution to this issue is converting the network itself to all Internet Protocol interconnection and that these proposals are not only redundant but wasteful. “If we are going to all IP, why do we need this?” “I’m expending my precious capital expenditures on my network ONCE… not twice!” “How do I make this abomination go away?”

TDM is not going away in the UK, Canadian or United States networks anytime soon. The solution may be better to insert a Media/Signalling gateway between the TDM switch and the edge Session Border Controller that can actually make the STIR/SHAKEN attestation. Refer to the following diagram.



[46] https://datatracker.ietf.org/doc/draft-ietf-stir-oob/history/

Some operators such as TELUS have experimented on whether a voice signal/announcement of "Call Authenticated" before the call is connected might be appropriate.[47]

5.15. Remediation in the event of a False Positive during the CLI Authentication.

Within the 4th FCC Report and Order on robocalls, there is a grey area that has yet to be resolved.

> "Second, we expand our safe harbor to include network-based blocking based on reason analytics that incorporate caller ID authentication information designed to identify calls that are highly likely to be illegal, if this blocking is managed with human oversight and network monitoring sufficient to ensure that blocking is working as intended. Third, we require that voice service providers that block calls disclose such blocking, establish a dispute resolution process to correct erroneous blocking, and promptly resolve disputes."

In practice, the dispute resolution procedure has not been fully implemented by some operators nor has there been a "one stop" procedure to permit a calling party to alert all the various providers that there has been an error.

6. FUTURE TECHNICAL DIRECTIONS IN STIR/SHAKEN BASED CLI AUTHENTICATION RICH CALL DATA TO DISPLAY

The ATIS SIP Forum Network to Network Interface Task Force and the IETF are working on implementing a further STIR/SHAKEN enhancement known as Rich Call Data (RCD).[48] This technology will permit originating service providers to not only validate the originating call identity, but transmit a rich set of data about the calling party validated by using the same STI-GA/PA infrastructure. This could include extensive name, address and contact information, as well as company logos, theme songs, etc., that could be displayed to encourage the consumer to actually answer the call. It is envisioned that this could be used by financial services firms to alert consumers to possible fraud, notification of pizza delivery, public service announcements on possible weather threats, or assist doctors' offices in reaching patients. The possible applications are endless. The beauty of Rich Call Data is that it could the same chain of trust that STIR/SHAKEN brings to Call Authentication.

[47] https://www.telus.com/en/about/news-and-events/media-releases/spam-calls-are-officially-a-thing-of-the-past

[48] https://datatracker.ietf.org/doc/draft-wendt-sipcore-callinfo-rcd/

It is strongly believed by all commentators to this report that RCD is a foundational technology and could alleviate the strong drop in call completion rates the industry has experienced and cost factors in Call Centers.[49]

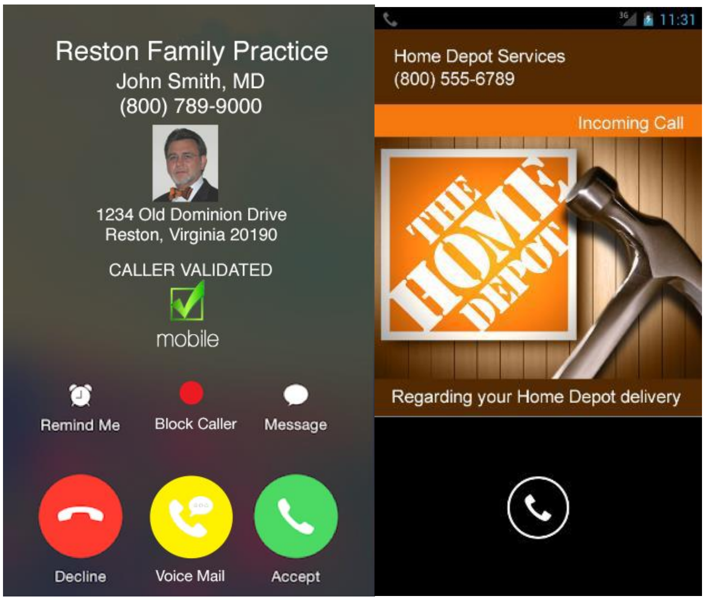
This is vitally important to UK Voice Service providers since the UK, or for that matter, most of Europe did not deploy CNAM (Calling Name Delivery). CNAM is an SS7 service that displays a 15-character ASCII string on a phone display.[50] It is an extremely popular service in the United States and Canada. Consumers can simply look at their telephones and decide whether they wish to answer the call or not based on a verbose name of who is calling.

Today, many network operators display UNKNOWN, for instance, when they do not have accurate data on either the Calling Party ANI or CNAM.

In the SS7 world, the CNAM service is a *terminating carrier* service, meaning that the terminating network operator must perform the lookup before the call is placed. Typically, this is a *TCAP* query to the originating carrier's *LIDB* service; however, several third-party vendors have emerged that create their own CNAM databases that competitive network operators can then use to look up the data. In SIP/IMS, this is reversed, and the verbose CNAM data can be delivered in the originating SIP INVITE message by any of several means.

As of now, CNAM is nothing more than fifteen characters of ASCII. In the modern age, this seems absurd, and logically should change.

Examples of Rich Call Data:



[49] https://www.callcenterhosting.com/blog/call-center-metrics-2020-for-businesses/
[50] Cisco (2007), http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/pgw/9/feature/module/9-7_3_/cnam.html.

Many United States and Canadian cable operators are considering deploying RCD technology in their Hybrid Fiber Co-Axial networks where the data could be displayed on the television screen.

Some vendors have referred to this opportunity as “Call Branding”, “Registered Caller” or “Free Caller Registry”, and multiple product offerings are being designed and offered.[51] [52] [53] [54] [55] The business case for these services is to attempt to reassure the consumer that the call is legitimate and that they should answer the call. The success of these offerings is unclear as of the date of this report.

6.1. Issues with Call Branding and Registered Caller and other forms of Caller Registration.

Issues with Call Branding and Registered Caller generally surround the issue of Identity management and how does the RCD data become distributed to the service provider so that they can utilize it. Is it distributed or must the data reside with the Service Provider? Who is responsible for vetting the data to be distributed in Rich Call Data? How do you promote interoperability and adoption? Will device manufacturers cooperate?

7. THE ROLE OF STIR/SHAKEN IN TEXT MESSAGING

The FCC Second Report and Order specifically expands the scope of Call Authentication to text-based messaging. To implement the Act’s new anti-spoofing provisions, the FCC

[51] https://www.home.neustar/trusted-call-solutions/branded-call-display

[52] https://www.hiya.com/products/connect

[53] https://firstorion.com/call-enhancement/

[54] https://registeredcaller.com/

[55] https://www.freecallerregistry.com/fcr/#

specifically defines “text message,” “text messaging service,” “voice service,” “caller identification information,” “caller identification service,” “short message service” (“SMS”) and “multimedia message service” (“MMS”). A careful reading of these definitions is critical to understanding which entities are covered under the new rules. As indicated in Section 64.1600 of the FCC’s Rules, “text message” for anti-spoofing purposes is defined as a “message consisting of text, images, sounds, or other information transmitted to or from a device that is identified as the receiving or transmitting device by means of a 10-digit telephone number or N11 service code.” The FCC defines “N11 service code” as an abbreviated dealing code that allows telephone users to connect to a network node by dialling only three digits (if the first digit is not 1 or 0); *e.g.*, 911 or 411. There is ample evidence that as the “noose tightens” on robocalls in the Voice Service, the perpetrators of fraud have moved to the SMS service.[56]

8. INTERNATIONAL COORDINATION WITH OTHER NATIONAL REGULATORY AUTHORITIES

In discussion with various commentators, it is recommended that OFCOM renew any existing Memoranda of Understanding with its regulatory colleagues at the FCC and the CRTC. The FCC has already signed an agreement with ACMA, the Australian Regulator.[57] There is anecdotal evidence that the robocalls have also spread to France and elsewhere.[58] There has already been considerable technical discussion on how the various STIR/SHAKEN root Certification Authorities could exchange data in order to facilitate interoperability.[59] This is an ongoing discussion that needs to proceed as soon as possible.

9. RECOMMENDATIONS: OFCOM’S COURSE GOING FORWARD

The Caller ID spoofing problem is a complex and multifaceted problem as noted. OFCOM’s decisions also influence the pace of change. It is vitally important that UK Voice Providers and OFCOM do not unrealistically raise expectations that the problem can be solved in the immediate future. It is vitally important that the pace of change be concurrent with the overall integrity and stability of the UK Voice Network.

[56] https://www.consumer.ftc.gov/articles/how-recognize-and-report-spam-text-messages

[57] https://www.fcc.gov/document/fcc-signs-robocall-enforcement-mou-australian-partners

[58] https://blog.hiya.com/robocalls-skyrocket-globally-growing-325-85-billion-worldwide-2018/

[59] https://datatracker.ietf.org/doc/draft-burger-stir-iana-cert/

The current plan to migrate the UK Voice Network to all Internet Protocol by 2025 is perhaps the best first step, but clearly will impose significant network and financial burdens on UK Operators.

It is likely that UK Operators' concerns will have far more to do with the costs they incur to upgrade their internal *Operational Support Systems (OSS)* and *Business Support Systems (BSS),* than those associated with the CLI Authentication solution itself.

The UK has chosen, for a variety of historical reasons, not to deploy Centralized Numbering Databases (CDB) for any numbering function. This poses some major challenges for full implementation of STIR.

Any implementation of techniques to mitigate CLI Spoofing should strive either to improve the ease with which LNP (which is closely related to the VoIP spoofing problem) is implemented, or at least, following the oath of Hippocrates to "do no harm".

There is no question that the deployment of a CLI Authentication solution for the United Kingdom will ultimately be linked with the structure and usage of the UK Numbering Plan and with future UK requirements for *Local Number Portability (LNP)* databases for the fixed and mobile network, as well as with Internet Protocol-based *Network-to-Network Interfaces*.

9.1. Proceed with All Deliberate Speed.

Given the state of the UK Voice Network, there is no reason not to proceed with the establishment of a UK Secure Telephone Identity (STI) Governance Authority for CLI Authentication at the earliest possible date. This report outlines the probable governance issues OFCOM will confront. There is ample evidence that there is sufficient Internet Protocol SIP/IMS and Internet Protocol interconnection in the UK network to provide real and tangible benefits to UK Consumers in advance of the full transition to IP. It is reasonable and prudent to gain all the advantages of STIR/SHAKEN -- even for a limited subset of UK consumers -- even if some elements of the UK network will not be able to fully implement it for some time.

9.2. STIR/SHAKEN is a Work in Progress.

OFCOM and UK Voice Operators need to understand that the CLI Authentication situation in the United States and Canada is still fluid and may see substantial modifications over the coming months and years as deployments proceed.

9.3. Develop a National UK Numbering Database.

It is the author's strong opinion that, in parallel to the implementation of CLI Authentication for the UK numbering plan, OFCOM should consider a major consultation among all stakeholders on how centralised numbering databases (CDBs) could be implemented addressing a variety of issues. NICC has already made preliminary determinations on the need for CDB for LNP among others and is well equipped to render appropriate standards through its Number Porting Steering Group. The time to act is now. The United States, Canada and other European nations have over twenty years of experience in the management and deployment of CDBs and their value cannot be underestimated. In particular, the author recommends looking at the remarkable work done by COIN in the Netherlands.[60]

9.4. No Support for TDM/SS7 Networks.

OFCOM and UK Service Providers SHOULD NOT entertain proposals for Out of Band CLI Authentication. It is redundant given the 2025 roadmap for All Internet Protocol implementations.

9.5. Establish a Policy on Call Blocking.

OFCOM will have to confront policy issues surrounding Call Blocking by UK Operators and under what terms, conditions and modifications of its rules regarding “Safe Harbor” (or its UK equivalent) should it decide to allow blocking.

9.6. Establish Guidelines on CLI Display.

UK Operators, at the explicit encouragement of OFCOM, should cooperate with all relevant technical standards bodies to implement Rich Call Data in their networks on how VERISTAT and Rich Call Data should be displayed to consumers and passed through to UK Enterprises. As previously noted, this represents a possible commercial opportunity for UK Operators.

9.7. Establish Traceback.

UK Operators, at the earliest possible date, should self-form a UK Traceback Consortium to assist OFCOM and UK Law Enforcement in understanding where the offending traffic is coming from. OFCOM may have to consider using its authority under its General Conditions Authority to shut down interconnection from UK Operators that refuse to enable its policies.

[60] https://coin.nl/en/home

9.8. Continue to Work with NICC.

The role of NICC Standards in the deployment of CLI Authentication and other network standards is vital. NICC is an essential part of the Standards Landscape in the UK. Its report on the Implementation of STIR in the UK is an essential document to understand. It is well researched and contains a deep understanding of the STIR/SHAKEN framework. OFCOM will need to engage NICC to extend this work as the implementation of STIR proceeds.

The timetables for all of these initiatives are difficult to determine and even in the United States and Canada there is ample evidence that some deadlines may be missed or modified given the enormity of the task at hand.

APPENDIX A: ABOUT THE AUTHOR

Richard Shockey has over twenty years of experience in various aspects of the telecommunications industry focusing on the use of Internet Protocol Technology for various forms of real time communications, specifically voice and messaging. He is an expert on Next Generation Network Signalling, the Session Initiation Protocol (SIP),[61] ENUM,[62] Voice Over Internet Protocols (VoIP), Voice Using Internet Protocols (VuIP), and various PSTN Transition Issues, including Robocall and Caller ID spoofing. He has advised telecom firms, governments, as well as several companies in the financial services industry on these matters.

Since 2007, Mr. Shockey has been Chairman of the Board of the SIP Forum.[63] The SIP Forum is an industry association with members from the leading IP communications companies. Its mission is to advance the adoption of IP communications products and services based on SIP. The Forum promotes SIP as the technology of choice for the control of real-time multimedia communication sessions throughout the Internet, corporate networks and wireless networks. Membership consists of internationally recognized companies and institutions, including Microsoft, Comcast, Cox Communications, Bell Canada, Deutsche Telecom, Ribbon Communications, Columbia University and Georgetown University, among others. The function of the Chairman of the Board is to lead the overall direction of the Forum, including developing and managing its budget in conjunction with the SIP Forum Executive Director, creating and supervising technical initiatives, as well as being a spokesperson for SIP and the Forum throughout the industry. Among the SIP Forum's work is the development of SIPConnect, the most widely adapted profile for IP-PBX to service provider interconnection in the world. The SIP Forum and The Alliance for Telecommunications Industry Solutions (ATIS) Joint Task Force have developed a national technical recommendation for All IP Network to Network Interconnection and jointly continue to advance the STIR/SHAKEN Call Authentication Framework for combating Robocalls and Caller ID spoofing. The ATIS/SIP Forum STIR/SHAKEN Framework has been formally mandated by both the Federal Communications Commission (FCC) and the Canadian Radio-Television and Telecommunications Commission (CRTC).

Since 2015, Mr. Shockey has been a member of Federal Communications Commission, North American Numbering Council (NANC). NANC is a Federal Technical Advisory Council within the FCC Wireline Competition Bureau, whose mission is to provide recommendations,

[61] https://tools.ietf.org/html/rfc3261

[62] https://tools.ietf.org/html/rfc6116

[63] www.sipforum.org

advice and guidance to the FCC on the administration of telephone numbers within the North American Numbering Plan (NANP). The NANP includes the United States, Canada and several Caribbean nations. Current issues include National Geographic Number Portability and techniques to combat Caller ID Spoofing and Robocalls. Mr. Shockey recently Co-Chaired the NANC Subcommittee to the Wireline FCC Competition Bureau on options to implement National Number Portability across the United States. From July 2011 to March 2013, he was a member of the Federal Communications Commission Communications Security Reliability and Interoperability Council (CSRIC). CSRIC is a Federal Technical Advisory Council within the FCC Public Safety and Homeland Security Bureau, whose mission is to provide recommendations to the FCC to ensure, among other things, optimal security and reliability of communications systems.

APPENDIX B: COMPANIES INTERVIEWED FOR THIS REPORT

ATT (United States)

Bandwith.com (United States)

British Telecom (United Kingdom)

Canadian Radio-Television and Telecommunications Commission (Canada)

Comcast (United States)

Cellular Telecommunications Industry Association (CTIA) (United States)

Federal Communications Commission (United States)

First Orion (United States)

Hiya (United States)

Iconectiv (United States)

Lumen (United States)

Metaswitch (United States)

NetNumber (United States)

NeuStar (United States)

Ribbon (United States)

Rodgers (Canada)

SecureLogix (United States)

Telus (Canada)

Transaction Network Solutions (TNS) (United States)

Verizon (United States)

Virgin Media (United Kingdom)