Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of:	)	
	)	
Protecting Consumers from One-Ring Scams	)	CG Docket No. 20-93
	)	
To: The Commission	)	

NOTICE of PROPOSED RULEMAKING FCC 20-57

Comments of the Risk & Assurance Group

Introducing the Risk & Assurance Group (RAG) and RAG's Wangiri Intelligence Exchange

RAG is a nonprofit international body of risk managers working in the telecommunications sector. Our mission is to provide educational and networking events for telco risk professionals around the world, sometimes leading to collaborative programs of work that tackle specific issues. In recent years we have run international conferences hosted by major telcos in Australia, Bahrain, Canada, Germany, India, Kenya, South Africa, the UK and the USA. One-ring or wangiri fraud has been an important recurring agenda item for those conferences, partly due to the lack of a consistent industry response to this global challenge. This prompted RAG to launch in 2019 an anti-wangiri initiative that encourages telcos to freely and rapidly exchange intelligence about wangiri using blockchain distributed ledger technology.

59 telcos worldwide now belong to the RAG Wangiri Consortium, giving them free access to the intelligence exchange. The members of the consortium include a wide variety of electronic communications providers across every continent, including major international wholesale carriers, multinational retail telecoms groups, the largest wireless operator in India, and small national retail telcos with limited anti-fraud budgets. The consortium is also backed by some of the largest global suppliers of telecoms fraud management systems who are enhancing their existing products and services by integrating them with the wangiri intelligence exchange. The purpose of this submission is to argue against duplicating what the consortium has already achieved, and to argue for more telcos and vendors to build on the foundations we have established.

A Brief Explanation of 'One-Ring' or Wangiri Fraud

The 'one ring' scam relies on simple human curiosity to trick consumers into making expensive calls. The scam begins when a call is made to the victim's phone, often ending so soon

afterwards that it is impossible for the consumer to accept it. Such short calls may incur no charge for the party that dials it; scammers program robocallers to take advantage of a tiny but known lag between when a call is actually connected (which is a high priority for networks) and when the duration of the call is measured for charging purposes (a lower priority). A 'missed call' message will hence be presented on the victim's handset. Human nature leads the victim to return this call without considering how much it will cost them. The scammers profit by receiving a share of the cost of the victim's call. The scammer's business model hence relies upon:

1. Obtaining control of phone numbers which will generate revenue whenever they are called.
2. Placing a large number of robocalls to a wide array of potential victims in the hope of luring them to call back.
3. Using a variety of methods to fool victims into prolonging any calls they make to the scammer's numbers.

This fraud is commonly referred to as "wangiri" within the telecommunications industry. Wangiri is a Japanese term meaning "one and cut". It is believed that the scam was first identified by NTT, a Japanese telco, around the start of the century. The earliest versions of wangiri were devised by premium-rate sex lines seeking to fool Japanese consumers into calling them back[1]. Article 15 of Japan's Wired Telecommunications Act explicitly prohibits the use of automated equipment that dials phones and then "immediately terminate without making a call"; the penalty is imprisonment of up to one year or a fine of up to JPY 1 million. Though the wangiri scam originated in Japan, it has since become global and pernicious, and now commonly involves luring the victim into calling an international destination.

There are several variations of wangiri fraud. For example some forms are targeted at enterprises that routinely return calls from customers. Calls made to these enterprises will deviate from the one-ring pattern because the fraudster's intention is to connect to the victim's voicemail or automated response system in order to leave a short message or to choose a menu option that will encourage a return call. Some fraudsters are willing to incur the cost of a call to their victim when there is a high likelihood of a return call. What is common to all versions of wangiri fraud is that a telephone number must be used by the scammer as bait for a return call.

It is to the advantage of the scammers to receive their profits in a different country to their victims, or at least to make their whereabouts obscure, in order to discourage action by national regulators and law enforcement agencies. We believe that the limited intelligence available to some telcos leads them to incorrectly believe that scammers tend to be based in the same country as their business and their customers, whilst the global patterns of fraudulent traffic argue otherwise. There is no good reason to believe that a scam which originated in Japan and which plagues customers in every country is only conducted by fraudsters located in the USA.

[1] https://www.economist.com/business/2002/10/03/youve-got-my-number

On the contrary, there is every reason to believe that fraudsters could easily relocate their base of operations from one country to another whilst continuing to exploit phone users everywhere. This means the problem of wangiri demands a global response.

Some national telecommunications providers and international carriers may feel little incentive to reduce wangiri because they also profit from the calls made by victims. This has slowed the industry's response to the growth of wangiri and discouraged collective action. However, it should also be noted that a few providers now actively seek to reimburse consumers without waiting to receive a complaint from them, although those telcos may not be able to avoid the wholesale cost of the call to themselves.

The Scale of the Global Problem

There has been a sharp and global rise in wangiri since 2017. This is related to the transition to IP networks, which has made it easier and cheaper for scammers to make all kinds of nuisance robocalls. Some types of telecoms fraud are targeted at wealthy customers, or customers in particular countries, but our research finds that wangiri fraudsters will indiscriminately call anyone with a phone, including residents of the world's poorest countries. This is corroborated by the wide variety of countries that have reported spikes in wangiri activity, which we will refer to as wangiri attacks.

RAG has monitored the web for warnings about wangiri attacks since late 2017. Our research shows that most countries have moved through two stages of explaining the problem to consumers:

- The initial phase occurs in response to a large and novel attack that affects a great many customers during a short space of time. The public are warned about the dangers of wangiri, and are told to avoid returning calls to specific numbers or to specific ranges of numbers associated with particular countries. Both regulators and telcos make announcements designed to reduce the number of returned calls and to allay fears that phones have been 'hacked' or that the fraudsters know about the recipients of missed calls. The FCC is just one of many national regulators that has found it necessary to issue such warnings.
- Whilst preventative measures and greater consumer awareness mean subsequent attacks may be less effective, an ongoing program of consumer education is needed. Press coverage is less alarmist in tone. Regulator warnings no longer mention specific numbers to avoid because it is understood that the fraudsters will vary their attacks and could use number ranges associated with many countries.

We believe that the following list is a subset of all the wangiri attacks that the public have been warned about since RAG began monitoring wangiri announcements.

- Australia, May 2018[2]
- Belgium, September 2019[3], February 2020[4] and May 2020[5]
- Canada, February 2018[6]
- Costa Rica, January 2020[7]
- Czech Republic, October 2019[8]
- Finland, February 2020[9]
- Guam, October 2018[10]
- Hong Kong, June 2018[11]
- Hungary, January 2019[12] and September 2019[13]
- Indonesia, March 2018[14]
- Ireland, October 2017[15] and February 2020[16]
- Italy, October 2019[17]
- Japan, November 2019[18]
- Kenya, February 2020[19]
- Lithuania, May 2020[20]
- Luxembourg, February 2019[21]
- Namibia, February 2018[22]
- Nepal, August 2019[23]
- Netherlands, October 2019[24]
- New Zealand, October 2019[25]

---

[2] https://www.news.com.au/technology/gadgets/mobile-phones/wangiri-calls-continue-to-target-aussie-mobile-users/news-story/5fa5a9fd91256a4d84ec01f0505344aa

[3] https://www.hln.be/nieuws/binnenland/opgelet-voor-telefoontjes-uit-paradijselijke-oorden-nummers-lijken-uit-zone-brussel~a4b017949/

[4] https://radio2.be/de-inspecteur/nu-ook-telefoonfraude-vanuit-spanje-verrassend-want-in-het-verleden-opereerden

[5] https://www.politie.be/5363/vragen/misdrijven-op-het-internet/je-ontvangt-bel-mij-smsjes-van-buitenlandse-nummers-wangiri

[6] https://www.vancourier.com/news/phone-scam-warning-don-t-return-a-missed-call-you-don-t-recognize-1.23168404

[7] https://www.cpic.or.cr/Posts/Details/Wangiri%20%E2%80%93%20Una%20de%20las%20modalidades%20de%20estafa%20telef%C3%B3nica

[8] https://twitter.com/Vodafone_CZ/status/1188008848801619968

[9] https://www.somic.fi/wangiri/

[10] https://www.ghs.guam.gov/community-urged-refrain-calling-back-international-phone-number-scam-could-result-high-rate

[11] https://www.scmp.com/news/hong-kong/hong-kong-law-and-crime/article/2150123/are-hongkongers-finally-learning-their-lesson

[12] https://bbj.hu/business/wangiri-phone-scam-on-loose-again_160794

[13] http://www.police.hu/hu/hirek-es-informaciok/bunmegelozes/aktualis/ismeretlen-kulfoldi-telefonszam

[14] https://news.detik.com/berita/d-3946176/wangiri-penipuan-bermodus-missed-call-misterius-dari-luar-negeri

[15] http://www.independent.ie/business/technology/wangiri-phone-scam-sweeping-across-ireland-is-unprecedented-say-operators-36240323.html

[16] https://www.corkbeo.ie/news/local-news/fresh-wave-fake-bank-scammers-17677748

[17] https://gazzettadelsud.it/articoli/societa/2019/10/17/truffe-telefoniche-con-chiamate-mute-dalla-tunisia-ecco-come-difendersi-7f5d6d34-18b2-42b0-ae43-926ea40fd6df/

[18] https://www.nishinippon.co.jp/item/n/561530/

[19] https://nairobinews.nation.co.ke/editors-picks/here-is-why-you-may-have-been-receiving-strange-calls

[20] http://udiena.lt/aktualijos/item/13936-nauja-wangiri-telefoniniu-sukciu-atakos-banga-lietuvoje-kas-tai-ir-kaip-apsisaugoti

[21] https://today.rtl.lu/news/luxembourg/a/1301022.html

[22] https://economist.com.na/33149/extra/telecom-companies-warn-of-wangiri-long-distance-calling-scam/

[23] https://www.nepalitelecom.com/2019/07/nta-warns-fake-missed-calls-wangiri-scam.html

[24] https://www.rtlnieuws.nl/nieuws/nederland/artikel/4889671/wangiri-fraude-opgelicht-slachtoffers

[25] https://www.facebook.com/spark4nz/posts/2757813284238493

- Norway, November 2018[26]
- Pakistan, May 2019[27]
- Poland, May 2020[28]
- Romania, October 2019[29]
- Slovakia, September 2019[30]
- Trinidad and Tobago, October 2019[31]
- United Arab Emirates, June 2018[32]
- UK, September 2019[33]
- USA, May 2019[34]

We believe many telcos fail to appreciate the true extent of the short abandoned calls instigated by wangiri fraudsters and carried by their networks. Others are unwilling to talk publicly about the scale of the problem. However, some telcos have gone on the record about how severe wangiri has become, and the number of fraudulent calls they automatically block. Telia, the international Tier 1 network headquartered in Sweden, announced in September 2019 that they had implemented a wangiri blocking solution that blocked "over a million calls per week"[35]. The CEO of Australia's largest telco, Telstra, published a social media post that discussed wangiri, saying that "in July [2019] alone we blocked 2.9 million scam calls"[36].

Taken together, we believe the surge in warnings and the number of calls being blocked by leading operators shows that wangiri fraudsters have the resources to launch enormous attacks at the customers of any telco in any nation. They have the resources to do this because they have profitably exploited the customers of those telcos that do not intervene to detect and prevent wangiri. Fraudsters have a strong economic incentive to keep launching attacks, even if their returns diminish as telcos improve their controls. The bulk of the cost to the fraudster is consumed by their capital outlay on equipment, whilst the operating costs are low and they face a negligible risk of punishment.

Preventative Controls

The technical and administrative controls that have been used to prevent wangiri fall into two categories:

---

[26] https://www.lofotposten.no/politi/svindel/mobiltelefon/politiet-advarer-mot-wangiri-svindel/s/5-29-427770
[27] https://www.dawn.com/news/1483672/premium-phone-call-scam-wangiri-does-the-rounds-in-pakistan
[28] https://www.telepolis.pl/wiadomosci/bezpieczenstwo/t-mobile-seniorze-uwazaj-na-te-numery
[29] https://evz.ro/alerta-pentru-romani-poti-ramane-imediat-fara-bani-nu-sunati-inapoi-la-aceste-numere.html
[30] https://www.bumm.sk/krimi/2019/09/07/gyanus-kulfoldi-telefonhivasokra-figyelmeztet-a-rendorseg
[31] http://www.looptt.com/content/customers-urged-ignore-missed-calls-foreign-numbers
[32] https://www.arabianbusiness.com/technology/398086-etisalat-issues-warning-over-phone-phishing-scam
[33] https://www.ofcom.org.uk/about-ofcom/latest/features-and-news/advice-wangiri-missed-call-scams
[34] https://docs.fcc.gov/public/attachments/DOC-357304A1.pdf
[35] https://www.teliacompany.com/en/news/news-articles/2019/wangiri-scams/
[36] https://www.linkedin.com/pulse/tackling-changing-face-our-customer-andrew-penn/

- Stopping the fraudster's initial call from being connected or stopping phone users from returning calls to the fraudster's number.
- Preventing the monetization of scams by denying fraudsters control of phone numbers they can profitably exploit.

Raising customer awareness also mitigates wangiri fraud.

Call Analysis

The best known control against wangiri, and the most impactful in terms of the number of calls affected, is based on simple data analysis. Because it is known that the scam typically begins with a large number of short abandoned calls, telcos should be able to identify an anomalous spike in their call patterns. Telcos may then block further calls from the same origin, or they may divert calls from that source to an automated voicemail system instead of connecting them to customers. Other telcos allow the calls to be connected to the customer, but they prevent the customer from calling it back.

The telcos who have implemented such controls have undoubtedly reduced the extent of wangiri suffered by consumers. However, data analysis is never perfect. For example, these techniques will never be effective at identifying the first call in an attack from a new source, because the pattern only becomes evident when there have been numerous anomalous calls. The telco needs to exercise judgment about when a pattern of fraudulent behavior has been demonstrated, and some customers will receive calls from fraudsters until that pattern is identified. Otherwise there would be a risk of blocking genuine calls and callers.

There is also evidence that once telcos successfully use data analysis to block calls then some fraudsters will respond by varying their techniques to evade detection. For example, it should be straightforward for telcos to identify a large spike in short abandoned calls made to numbers nnn-nnn-nnn1, nnn-nnn-nnn2 etc in sequence, but other patterns will be more difficult to identify. Fraudsters can reprogram automated diallers to make calls less frequently, and to dial numbers that follow a less obvious sequence. Other variations of the wangiri scam are even harder to detect. For example, there have been reports of wangiri-like scams that target enterprises which run call centers with automation designed to routinely call customers back[37] [38].

Allocation of Phone Numbers and Routing

The fraudulent abuse of telephone numbers is not limited to wangiri. There are several other types of fraud where the monetization depends on controlling the telephone numbers used to receive calls. These are two common examples:

[37] http://bswan.org/business_victim_wangiri.asp

[38] https://iconectiv.com/news-events/safety-numbers-fighting-fraud-job-everyone-says-iconectiv

- The call is to a premium-rate number, where an unusually high termination fee is charged by the recipient communications provider. This fee is split by the provider and another business which supposedly provides a service using this phone number. The original wangiri scam involving Japanese sex lines was monetized in this fashion. The telecoms industry has gone to considerable effort to curtail the abuse of premium-rate numbers, but it still persists.
- Another approach to monetization requires numbers to be incorrectly routed or 'short-stopped'. A call that needs to be routed through three or more networks in order to reach its proper destination is misdirected by a dishonest intermediary carrier to a voicemail system instead of being passed on to the next telco. This can be lucrative because the originating telco will pay the rate associated with an expensive final destination, as occurs with some remote islands, but the dishonest intermediary carrier keeps all of this fee without incurring any charge for passing it on. The dishonest carrier splits the proceeds with their accomplices.

The work that is done to reduce these abuses is extensive and should be commended. However, the industry has never been able to eliminate the abuse of numbers and routing entirely, and is unlikely to do so in the near future. Like a chain, the management of telephone numbers and the routing of calls is only as secure as its weakest link. Fraudsters may only need to corrupt key staff working for a national regulator or a telco for a short period in order to launch a lucrative string of wangiri attacks during their window of opportunity.

Protocols like STIR/SHAKEN that authenticate the origin of a call will likely reduce frauds where criminals spoof numbers. However, not all wangiri numbers are spoofed, and the adoption of STIR/SHAKEN will not eliminate wangiri if implemented in isolation. The number ranges already being exploited by fraudsters belong to countries who will be last to upgrade to the IP networks needed to support STIR/SHAKEN. These countries will also be amongst the last to adopt any other protocol for authenticating numbers, by virtue of their relative poverty. Some telcos in rich countries have been known to advocate the barring of calls to countries like these, but RAG considers that to be a mistake. Countries that have high termination rates for international calls often impose them because they are relatively poor and remote. Instead of punishing them for using international calls as a source of revenue, with a consequent increased risk of fraud by dishonest intermediaries, they should be helped to assist the fight against fraud by giving them affordable access to anti-fraud intelligence exchanges used by the telcos on both ends of each international call.

Customer Awareness

Whilst bodies like the FCC do what they can to advise customers, and whilst the work of journalists means the word 'wangiri' is now known to phone users worldwide, the simplicity of the scam means that it unlikely that this fraud can be eliminated solely by warning customers about the risks of returning a call to an unrecognized number. Methods to authenticate callers, such as STIR/SHAKEN, will reduce the risks for some kinds of customers. However, other

phone users, including businesses, expatriate workers and other consumers with families overseas will not be protected from the misuse of phone numbers associated with other countries.

The RAG Wangiri Blockchain: A Proven, Working, Inexpensive and Immediate Enhancement that Could Evolve into the Basis for a Permanent Solution

As described above, the most successful control that telcos have implemented to reduce wangiri relies on analyzing data to identify anomalous patterns of calls indicative of an attack by a fraudster. RAG's anti-wangiri initiative builds upon that foundation by applying a simple principle: *more data is always better than less data*. Some large international telcos, such as Vodafone Group, have implemented cross-border solutions that collate wangiri data from multiple operating companies in order to more rapidly identify each new attack. Other international carriers refer to their size and hence to the amount of data they accumulate as a reason for retail telcos to purchase their wholesale services; they acknowledge that their size gives them an advantage in identifying fraud. The RAG Wangiri Blockchain recreates the advantages of scale by providing an inexpensive, simple, distributed and near real-time mechanism for telcos to share their data.

To elaborate on an example given above, no telco can identify a wangiri attack from the *first* call of an attack from a new source. But what if another telco in the same country had just been subjected to a wangiri attack from that number, or from similar numbers? Whatever thresholds that the telco chooses to apply when looking for anomalous patterns, it follows that they should be more sensitive to calls that repeat the patterns of attacks recently suffered by other telcos. Put simply, having access to the data supplied by other telcos means they do not need to wait so long, or allow the attacker to make as many calls, before they can identify patterns indicative of wangiri. They can hence take action sooner, and reduce the losses suffered by their customers.

It is an open secret that some telcos will not spend a penny on protecting customers from fraud until they are mandated to do so. If they do spend money, the priority is to protect their own customers, not the customers of other telcos. These factors can make it difficult to pursue novel collaborative solutions on a voluntary basis, and they help organized criminals to keep making money by repeating the same fraudulent schemes. That is why RAG has eliminated cost as a barrier to the adoption of the RAG Wangiri Blockchain by giving free access to telcos that share their intelligence. There is no need to purchase hardware to access the wangiri blockchain; approved users can choose to access the ledger through a web portal. The only participants who must pay for access are those who would otherwise be freeriders, by taking data without providing any.

Granting free access to telcos who upload their data has enabled RAG to obtain the support of 55 retail telecommunications providers and 4 wholesale telecommunications carriers, all of whom have joined our wangiri intelligence sharing consortium since formal admission began in

February 2020. The participants in the consortium include: Vodafone, a large international retail group and wholesale carrier; iBasis, one of the world's largest international wholesale voice carriers; Ooredoo, a multinational retail telecoms group; Reliance Jio, an Indian retail operator with over 370 million wireless subscribers[39]; and a wide variety of smaller national retail telcos in various countries. The full list of participants is given in Appendix A.

Whilst the majority of consortium members are telcos who access the ledger through the web portal, we have also engaged with specialist suppliers of anti-fraud systems in order to further simplify and ease access for their telco customers. Subex and Neural Technologies, two of the largest suppliers of fraud management systems (FMS) to telcos globally, have recently completed development work to integrate their FMS products with the wangiri blockchain. This means that existing customers of their FMS will all be able to automatically share their own data, whilst utilizing the data provided by others to enhance the algorithms used to identify wangiri. We believe this will lead to a rapid expansion in the number of telcos participating in the exchange of data because these FMS suppliers have several hundred telco customers between them.

Other suppliers like GBSD Technologies have connected different anti-fraud products such as their automated blocking systems to the wangiri blockchain. This gives their customers the opportunity to automatically update the filtering of calls based on intelligence supplied by the consortium of telcos. RAG's strategy is to make wangiri intelligence available to specialist suppliers of anti-fraud systems so telcos can better protect customers by leveraging products and services they already use.

We expect that some large telcos will recommend that there is no need for information sharing in order to tackle wangiri fraud, but that is flawed advice. As noted above, large telcos enjoy a high degree of success in identifying anomalous patterns by extrapolating from the history of previous calls. However, the effectiveness of the same technique will be markedly less for smaller telcos because of the limited pool of historic data they possess.

We have also observed that some large telcos consider it is not in their interests to share data for *commercial* reasons. As described above, some large international wholesale carriers make reference to their ability to prevent fraud when marketing their services to other telcos. They are effectively seeking to charge a premium in exchange for enhanced fraud protection. Such carriers will openly state that it is advantageous to use their services because they can exploit a larger pool of data than their rivals. Though they would never admit it publicly, this makes some international carriers unwilling to exchange data, even though they may have agreed to comply with codes of conduct that state they should *proactively* share fraud intelligence of use to other telcos.

[39] https://www.trai.gov.in/sites/default/files/PR_No.29of2020.pdf

RAG believes that telcos should treat fraud prevention as a civic duty, and not as a source of competitive advantage. Participants in the wangiri intelligence exchange evidently feel the same way; their uploaded data will help others to tackle fraud. Though it might be seen as peripheral, the increasing volumes of certain kinds of fraud that affect consumers should also be treated as a potential source of anti-competitive behavior. A large telco which has both a retail consumer division and a wholesale carrier division would be able to leverage all of its data to best protect the customers of its retail consumer division. A small retail telco may be a competitor at one level whilst also being a customer for the large telco's wholesale carrier services. It would not serve the best interests of the public if the customers of the small retail telco were less effectively protected from fraud because their wholesale partner did not use its data to protect them too. Nor would it be equitable to charge the small retail telco a higher rate in order to guarantee like-for-like fraud protection. That is why a simple, universal common repository for fraud intelligence will deliver better results for customers of all telcos than solely depending on large carriers to embed fraud management in the services they sell to other telcos.

The RAG Wangiri Blockchain uses proven and effective technology. 35 telcos and suppliers took part in a six-month pilot of the technology during the latter half of 2019, and the system suffered no downtime during that period. The production version that was launched in February 2020 has now been used to exchange information about more than 1 million distinct instances of wangiri. More than a billion consumers are served by the telcos that participate in the wangiri intelligence exchange. But the most exciting aspect of this initiative is its potential to evolve from a cost-effective enhancement of existing anti-wangiri controls into a mechanism that could rapidly determine the source of wangiri.

RAG would be glad to assist the FCC and other regulatory and enforcement bodies by providing data to assist any investigations into sources of wangiri fraud. It is our belief that a global ledger of wangiri, proactively compiled by reputable telcos, would greatly improve the efficiency of processes that otherwise rely on reactive queries to trace the origin of fraud. As noted above, all wangiri relies on exploiting a number that the fraudsters want victims to call. This would be the reliable 'key' to an efficient database query. The RAG Wangiri Blockchain is building the necessary database, which grows as each new telco joins the consortium.

Wangiri scammers, like other fraudsters, take advantage of the uncertainty created by multiple carriers being involved in the handling of a call from its origin to its destination. Because the RAG Wangiri Blockchain is an inexpensive and rapid way to collate data, it will provide an increasingly comprehensive 'map' of the flows of wangiri calls as more telcos exchange intelligence. The real source of a wangiri attack will want to remain obscure, but if every other telco that participates in the management of that call is also a participant in the wangiri blockchain then it will soon become evident which telcos are less effective at identifying wangiri. Progress in completing the map will clarify the actual sources of wangiri. Such a goal cannot be accomplished overnight, but eliminating cost and technical barriers begs a question about the motives of those telcos which do not want to exchange intelligence, whilst avoiding all the usual arguments against information sharing. The more comprehensive our map of wangiri, the

quicker and easier it will be to draw conclusions about bad actors in the global telecoms ecosystem, making enforcement action more feasible than before.

Why Not?

It is our experience that if you consult the opinions of many telco fraud managers it will not take long to find someone who will argue *against* taking action. This is considered normal for a sector that routinely produces reports that fraud has a high cost, but which can struggle to respond both collectively and decisively. There will be different opinions as to why some telcos lack the appetite to reduce fraud. The rapid progress enjoyed by the RAG Wangiri Blockchain shows that great strides can be made if the telcos that want to work together are not held back by the telcos that prefer inaction. The first designs for the wangiri blockchain were written in early 2019; a working prototype was running by mid-2019; a successful pilot involving 35 businesses was completed at the end of 2019; lessons were learned and incorporated into a production version that launched in February 2020; and now there are 59 telcos actively using the technology to exchange data. All of this was accomplished with a shoestring budget and a lot of goodwill from fraud professionals who want to see positive change.

RAG's recommendation would not be to make the use of the RAG Wangiri Blockchain mandatory. We believe momentum is on our side, and more telcos will voluntarily choose to exchange intelligence simply because those who have not yet joined will increasingly see the benefits of pooling their data with a growing number of fellow telcos. All we ask is that consideration be given to our success to avoid an unhelpful duplication of effort.

Wangiri is a global problem, and it will be solved more adroitly if telcos on every continent see reasons to voluntarily exchange data without waiting to be told to adopt country-specific solutions. If the growth of the number of telcos using this intelligence exchange should stall in future, we will still have conducted a valuable learning exercise, not just in terms of the data collated about wangiri, but also about the factors that encourage or discourage telcos from working together to protect customers. The information obtained would then provide a much sounder basis for any subsequent regulatory intervention.

Submitted on behalf of the Risk & Assurance Group on June 18, 2020

Eric Priezkalns,
Chief Executive of the Risk & Assurance Group
eric.priezkalns@riskandassurancegroup.org
+44 7958 467273

Appendix: List of RAG Wangiri Consortium Members

Consortium Member Name	Entities	Telcos			Vendors	Date Joined
		Retail Telco	Subscribers (M's)	Wholesale Carrier		
Vodafone Group	29	28	625	1		Feb-20
Shaw / Freedom Mobile	2	2	5			Feb-20
YTL	1	1	1			Feb-20
Araxxe	1		N/A		1	Feb-20
LATRO Services	1		N/A		1	Feb-20
Epic	1	1	1			Feb-20
Colt	1		0.1	1		Feb-20
HT Eronet	2	2	0.5			Feb-20
Primetel	1	1	0.1			Feb-20
MTN Cameroon	1	1	7			Mar-20
MTN Nigeria	1	1	64.3			Mar-20
GO	1	1	0.5			Mar-20
Subex	1		N/A		1	Mar-20
Neural Technologies	1		N/A		1	Mar-20
Mascom	1	1	1.5			Apr-20
Algeria Telecom	1	1	3.8			Apr-20
GBSD Technologies	1		N/A		1	Apr-20
Entel	1	1	0.75			Apr-20
Vivacom	1	1	3			Apr-20
Megafon	1	1	77			Apr-20
MTN Guinea Bissau	1	1	0.6			Apr-20
Oordeoo Group	8	8	116.7			Apr-20
Globe Teleservices	1		N/A		1	Jun-20
Reliance Jio	1	1	370			Jun-20
iBasis	1		0.1	1		Jun-20
Zain Kuwait	1	1	2.5			Jun-20
SIGOS	1		N/A		1	Jun-20
LANCK Telecom	1		0	1		Jun-20
Yates Fraud Consulting	1		N/A		1	Jun-20
MTN Uganda	1	1	11.2			Jun-20
Total	**67**	**55**	**1,292**	**4**	**8**	