International Revenue Share Fraud (IRSF)

Understanding the value of International Premium Rate (IPR) Test Numbers

---

1. Introduction

The significance and impact of International Revenue Share Fraud (IRSF) to the telecommunications industry is well known. According to the Communications Fraud Control Association (CFCA) 2015 Global Fraud Loss Survey, IRSF is responsible for annual losses of $US10.8 billion, a 497% increase from the losses of $US1.8 billion in 2013.

Despite these losses, and the longevity of IRSF as a revenue stream for fraudsters, the problem remains and the increasing losses continue to frustrate the worlds operators. The industry has tried, and failed up until now to find a common solution to this problem, so most CSP's are developing and implementing their own solutions. Some of the solutions being implemented do not cover all areas of IRSF risk, for example introducing 24x7 monitoring of NRTRDE records will not identify an IRSF attack through a customers hacked PBX, or using the Fraud Management System to identify calls to high risk destinations will not quickly identify an IRSF attack through a roaming partner. Monitoring for calls to high risk destinations is unlikely to identify a Wangiri Fraud attack when multiple customers are making single calls. Some CSP's rely on country and number range blocking, however there are currently over 220 country codes being made available through the IPR Test Numbers being advertised, making them all high risk. Obviously it is not possible to block them all.

2. IPR Test Numbers

Irrespective of the method being used by the fraudster to carry out their IRSF attack, or the country being called, there is always one common factor in the fraud and that is the status of this number being called. In all IRSF attacks, the called number must be one that has the ability to generate revenue for the fraudster. In the majority of IRSF attacks, the Fraudster will want to confirm at least 2 conditions exist before starting the IRSF attack, which are;

- The IRSF number/s they wish to use can be called from the device and country they are calling from (that no blocking or restrictions are in place to prevent this), and
- The device they are using is capable of making multi-party calls (Smartphone features allowing up to 6 simultaneous calls from a single handset has been enabled)

To do this, they will (in most cases) go to the website of the IPRN Provider they intend using to obtain IRSF numbers from, and obtain test numbers to complete test calls to each country and number range they wish to target, before commencing the fraud attack.

The value of these test numbers as a fraud indicator is huge. Once they are known, they have the potential when used as a 'called number hotlist', to alert a Fraud Analyst to a potential IRSF attack before the call pumping activity commences. These test numbers may be anywhere between 30 minutes and 2 days prior to the IRSF attack getting in to full swing, and there is nothing else available to a CSP to consistently provide them with such valuable early warning of a potential attack to enable them to shut it down so quickly.

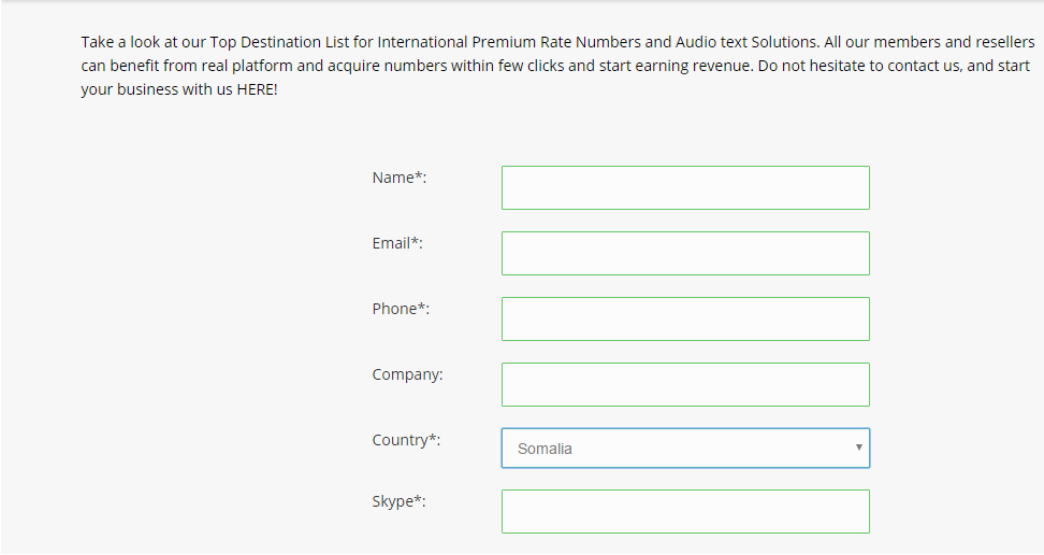
3. Case Study

This general case study intends to provide a clear understanding of how these test numbers are used, and the value that can be realised through using these as a 'called number' hotlist.

To demonstrate this value, we will use an actual IRSF case which occurred within the past 12 months. The fraudsters, through a carefully planned and executed fraud, obtained delivery of over 50 Simcards which were sent to them by the victim CSP in another country. Once the fraudsters received these Simcards, they executed the second phase of their operation which resulted in the Simcards being activated, with roaming enabled, without the CSP being aware. The activated Simcards were then ready to be distributed to the fraudsters associates who would be responsible for 'pumping' calls in to the IRSF numbers that would be provided to them. However, prior to this happening, the fraudster would have to confirm that each of the 50 plus Simcards was capable of calling the various countries he wished calls placed to, so this would require some test calls to be made.

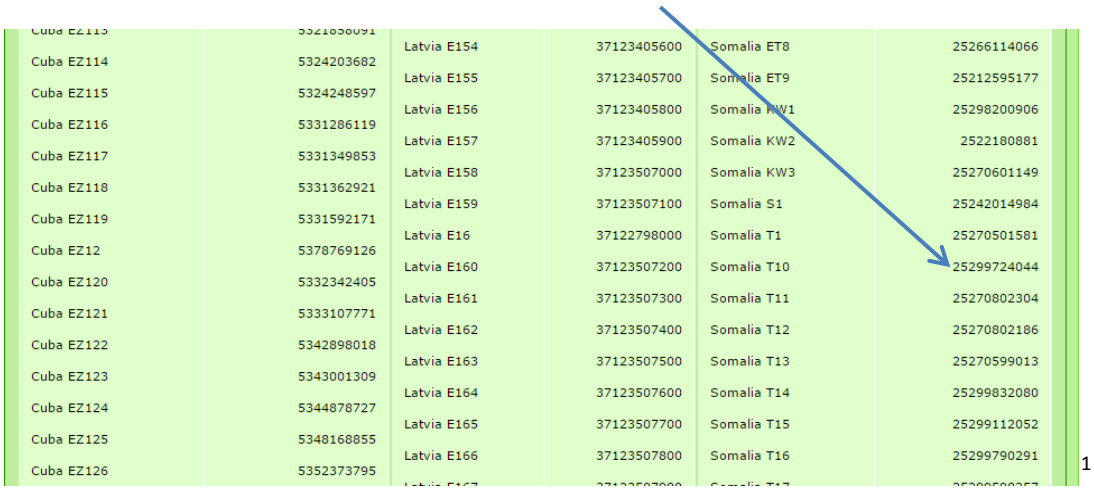
The process the fraudster would then follow is;

3.1 The fraudster is likely to have already decided which of the several hundred IPRN Providers they wished to deal with. To help make this decision he is likely to have gone to the IPRN Providers website and made a request for their rate card, so he could see what was on offer for the various countries he was interested in. A typical example of this application would be;



In this case, the fraudster has indicated that he is interested in numbers in Somalia so would have been provided with a payout rate to that country, which would have been in the region of 18 to 19 US cents per minute for every call he terminated.

3.2 Assuming that this rate was acceptable to the Fraudster he would have then gone back to the IPRN Website, and taken a Somalia test number being advertised by that IPRN Provider. One of the test numbers he has taken from the IPRN Providers website (Somalia 25299724044) is identified from their test numbers below;



Cuba EZ114	5324203682	Latvia E154	37123405600	Somalia ET8	25266114066
Cuba EZ115	5324248597	Latvia E155	37123405700	Somalia ET9	25212595177
Cuba EZ116	5331286119	Latvia E156	37123405800	Somalia KW1	25298200906
Cuba EZ117	5331349853	Latvia E157	37123405900	Somalia KW2	2522180881
Cuba EZ118	5331362921	Latvia E158	37123507000	Somalia KW3	25270601149
Cuba EZ119	5331592171	Latvia E159	37123507100	Somalia S1	25242014984
Cuba EZ12	5378769126	Latvia E16	37122798000	Somalia T1	25270501581
Cuba EZ120	5332342405	Latvia E160	37123507200	Somalia T10	25299724044
Cuba EZ121	5333107771	Latvia E161	37123507300	Somalia T11	25270802304
Cuba EZ122	5342898018	Latvia E162	37123507400	Somalia T12	25270802186
Cuba EZ123	5343001309	Latvia E163	37123507500	Somalia T13	25270599013
Cuba EZ124	5344878727	Latvia E164	37123507600	Somalia T14	25299832080
Cuba EZ125	5348168855	Latvia E165	37123507700	Somalia T15	25299112052
Cuba EZ126	5352373795	Latvia E166	37123507800	Somalia T16	25299790291

[1]

3.3 During this same phase of the fraud, the fraudster would have obtained other test numbers for other IRSF destinations, likely from the same IPRN Provider. Once he had sufficient test numbers, his call testing would begin.

3.4 In this case the test calls started at 8.50pm on the 5th day of the month of the fraud attack and as can be seen from a sample of the actual IRSF call records below, the first 4 calls were to a Liberia number. These 4 calls were in 2 stages, obviously to test that multi-party calling was permitted (first call established and put on hold when the second call was then made). Following this, a further 7 calls were made to the same Somalia number that had been identified from the IPRN Providers website. The first 6 of these calls were obviously made not only to confirm that calls could be made to Somalia, but also that the Simcard and device he was using allowed 6 simultaneous calls to be made to this destination (1st call made and put on hold, 2nd call made to same number and put on hold and so on – confirmed by the fact that 6 calls of over 1 minute duration were made within a 1 min 08 second time period.)

Calling number	Called Number	Date/time of call	Duration	Cost
XXX763014	23190387379	05/XX/20XX 8:50:57 PM	0:00:33	$3.87
XXX763014	23190387379	05/XX/20XX 8:51:04 PM	0:00:23	$3.87
XXX763014	23190387379	05/XX/20XX 8:53:03 PM	0:00:14	$3.87
XXX763014	23190387379	05/XX/20XX 8:53:13 PM	0:00:02	$3.87
XXX763014	25299724044	05/XX/20XX 8:56:34 PM	0:02:13	$9.68
XXX763014	25299724044	05/XX/20XX 8:56:47 PM	0:01:59	$7.74
XXX763014	25299724044	05/XX/20XX 8:56:53 PM	0:01:53	$7.74
XXX763014	25299724044	05/XX/20XX 8:57:21 PM	0:01:25	$5.81
XXX763014	25299724044	05/XX/20XX 8:57:27 PM	0:01:19	$5.81
XXX763014	25299724044	05/XX/20XX 8:57:42 PM	0:01:01	$5.81
XXX763014	25299724044	05/XX/20XX 9:02:31 PM	0:00:01	$3.87

[1] We make no suggestion that the operators of the websites from which the screenshots reproduced in items 3.1 and 3.2 above were taken, were involved in any way in the IRSF attack referred to in this paper.

3.5 In this prelude to the fraud attack, the pattern of test calls continued until 9.35pm, when traffic pumping in to Somalia IRSF numbers started in earnest. Test calls were also seen from the majority of the other Simcards in the possession of these fraudsters and during the 30 minute period from the first call at 8.50pm, 36 test calls were made from these Simcards.

This IRSF attack went undetected for 77 hours, concluding at 06.30am on the 9th of the month. This included a weekend, and during this period 605 unique numbers were called in 41 different countries with a total loss to the CSP of $US2.130 million. Call charges throughout the period of this fraud attack were averaging $US27,662.00 every hour. NRTRDE records were not being checked during this weekend period.

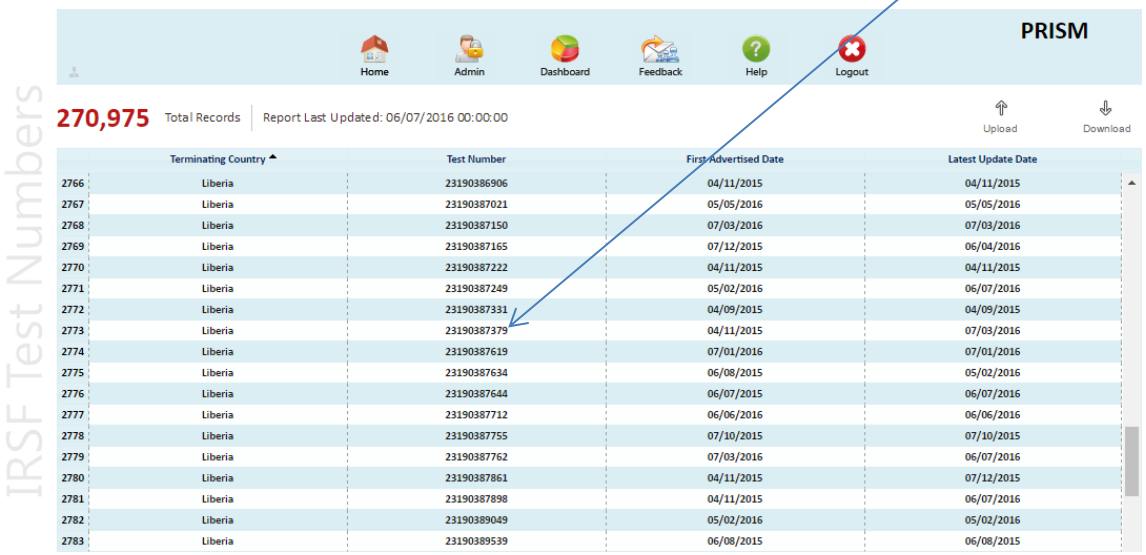
4. PRISM IPR Test Number Database - How these test calls have been detected:

The PRISM IPR Test Number database is now in its 3rd year of operation, and as at the 7th July 2016, contains almost 271,000 test numbers. These test numbers are obtained from the websites and rate cards of over 140 IPRN Providers. The database is updated every month, with between 12,000 and 17,000 new numbers being added with each update, as IPRN Providers change numbers to avoid them becoming known by CSP's. There is considerable effort put in each month by a team of analysts to source new IPR numbers and to maintain the database in a secure and trusted environment where those using the service can access the numbers, and update their own hotlists as the new numbers are made available each month.

Those CSP's who are now using PRISM as a 'called number hotlist' are unanimous in their praise of the IPR test number database as a tool to aid in the early detection of an IRSF attack. Some qualify this by adding that the database has proven it can identify up to 75% of their IRSF attacks, and is a key contributor to their IRSF prevention strategy.

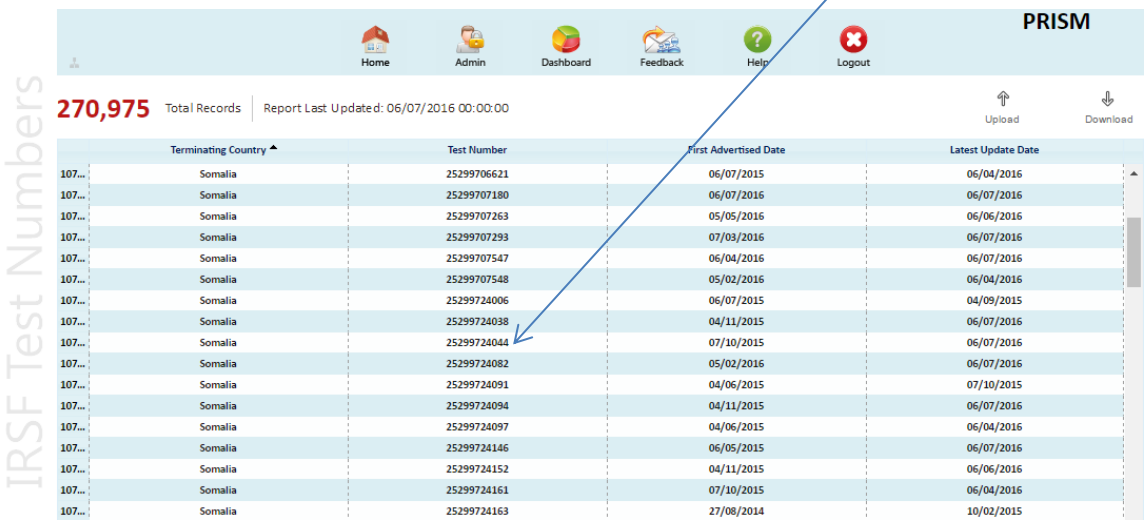
To establish how the IPR test Number database could have assisted in identifying this $US2.130 million IRSF attack is demonstrated in the two screenshots from the PRISM database below;

This screenshot shows some of the numbers in the database from Liberia. +23190387379 is the first test number called at 8.50pm on the 5th and this number is in PRISM.



	Terminating Country	Test Number	First Advertised Date	Latest Update Date
2766	Liberia	23190386906	04/11/2015	04/11/2015
2767	Liberia	23190387021	05/05/2016	05/05/2016
2768	Liberia	23190387150	07/03/2016	07/03/2016
2769	Liberia	23190387165	07/12/2015	06/04/2016
2770	Liberia	23190387222	04/11/2015	04/11/2015
2771	Liberia	23190387249	05/02/2016	06/07/2016
2772	Liberia	23190387331	04/09/2015	04/09/2015
2773	Liberia	23190387379	04/11/2015	07/03/2016
2774	Liberia	23190387619	07/01/2016	07/01/2016
2775	Liberia	23190387634	06/08/2015	05/02/2016
2776	Liberia	23190387644	06/07/2015	06/07/2016
2777	Liberia	23190387712	06/06/2016	06/06/2016
2778	Liberia	23190387755	07/10/2015	07/10/2015
2779	Liberia	23190387762	07/03/2016	06/07/2016
2780	Liberia	23190387861	04/11/2015	07/12/2015
2781	Liberia	23190387898	04/11/2015	06/07/2016
2782	Liberia	23190389049	05/02/2016	05/02/2016
2783	Liberia	23190389539	06/08/2015	06/08/2015

This second screenshot shows numbers in the database from Somalia. +25299724044 is the second unique test number called at 8.56pm on the 5th and this number is in PRISM



	Terminating Country	Test Number	First Advertised Date	Latest Update Date
107...	Somalia	25299706621	06/07/2015	06/04/2016
107...	Somalia	25299707180	06/07/2016	06/07/2016
107...	Somalia	25299707263	05/05/2016	06/06/2016
107...	Somalia	25299707293	07/03/2016	06/07/2016
107...	Somalia	25299707547	06/04/2016	06/07/2016
107...	Somalia	25299707548	05/02/2016	06/04/2016
107...	Somalia	25299724006	06/07/2015	04/09/2015
107...	Somalia	25299724038	04/11/2015	06/07/2016
107...	Somalia	25299724044	07/10/2015	06/07/2016
107...	Somalia	25299724082	05/02/2016	06/07/2016
107...	Somalia	25299724091	04/06/2015	07/10/2015
107...	Somalia	25299724094	04/11/2015	06/07/2016
107...	Somalia	25299724097	04/06/2015	06/04/2016
107...	Somalia	25299724146	06/05/2015	06/07/2016
107...	Somalia	25299724152	04/11/2015	06/06/2016
107...	Somalia	25299724161	07/10/2015	06/04/2016
107...	Somalia	25299724163	27/08/2014	10/02/2015

Calls in to both of these numbers would have generated 13 PRISM Test Number call alerts had these calls been monitored through the database, while 24 of the other 36 test numbers called during that first 30 minute period before this fraud attack moved to the traffic inflation stage would have generated multiple alerts. Throughout the period of this particular fraud, 289 fraud alerts would have been generated from calls to IPR test numbers as Fraudsters tested new countries during the fraud attack, had this CSP been using PRISM.

5. Conclusion

The value of utilising the IPRN database is completely unrelated to whether or not a CSP has 100,000 or 60 million customers. It should be viewed as a necessary insurance against significant IRSF losses. Other areas of business risk that could result in losses of the same significance as IRSF are generally managed through an investment to improve the control environment, and fraud prevention should be treated no differently. While the example provided in this case study is extreme, the investment required to utilise this database is low, and a significant return on that investment will be achieved if a CSP can identify and stop even a minor IRSF attack through the identification of Test Numbers being used.

If anyone is in any doubt of the value that can be achieved from utilising the IPR Test Number Database, you are welcome to send the writer the call records from your last 1 or 2 IRSF attacks. Once we have analysed these against the Test Number Database, we will be able to indicate at what stage of the IRSF attack fraud alerts could have been generated, and we are sure any doubts you have regarding the value of utilising these numbers will be put to rest.

Colin Yates

Colin Yates, CFE
Director and Principal Consultant
Yates Fraud Consulting Limited
30 July 2016