http://bswan.org/protecting_mvnos.asp

April 2015

Protecting 900+ MVNOs around the Globe from IRSF Fraud Pirates

interview with Colin Yates

Telecom fraudsters behave a lot like electricity: they follow the path of least resistance, gold being their favorite conductor of electrons.

And when it comes to International Revenue Share Fraud (IRSF) — a fraud that robs telecoms of a cool $4 billion a year — that new path of least resistance is the MVNO, the 900+ mobile operators who generally own no mobile networks, but sell mobile service virtually — reselling the facilities of a network operator.

That's the analysis of Colin Yates, a foremost consultant and authority on fighting IRSF fraud, and he's here to tell Black Swan readers all about this new threat — and explain what MVNOs should do to protect themselves.

Dan Baker: Colin, what's the scoop? What's changed to make MVNOs more susceptible to IRSF? And maybe we should change the meaning of the term MVNO to "Massively Vulnerable Network Operator".

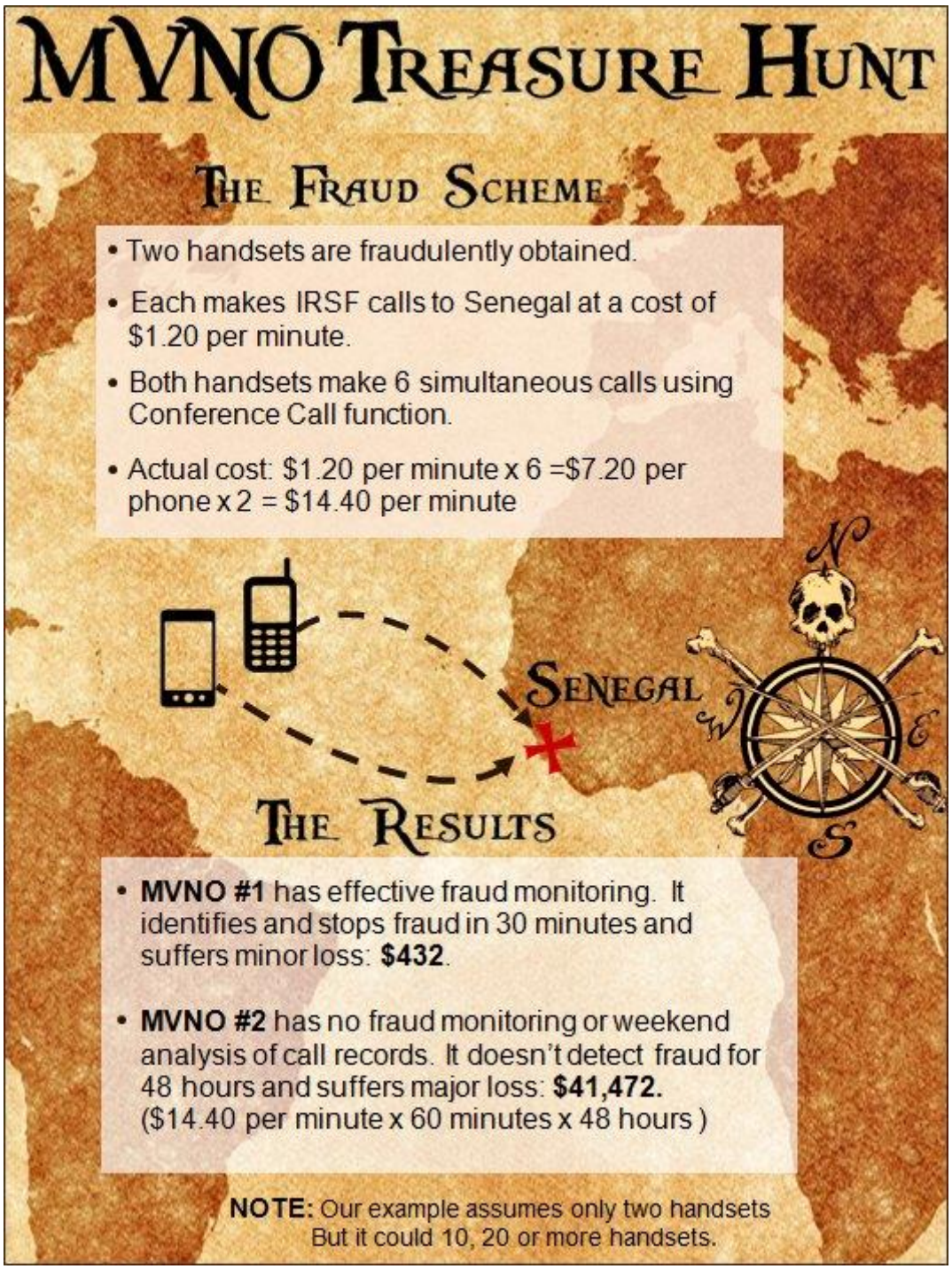
Colin Yates: Dan, the MVNOs definitely <u>are</u> massively vulnerable. Without fraud management domain knowledge, training, and tools, you're an easy target to be picked off by IRSF fraudsters. Data I've collected suggests that in the last 3 or 4 months there has been a gradual shift toward fraudsters attacking MVNOs more and more.

I think that's a conscious decision by the fraudsters. Mobile and fixed operators have suffered IRSF attacks for 7 or 8 years now, but over time they have become skilled at putting in controls for prevention and early detection.

Big damage has already been done. Last month I spoke to two MVNOs who suffered losses of around $500,000 each. And neither of them had any effective controls. One of those

MVNOs missed out entirely on the required knowledge transfer and intelligence around IRSF.

Now the mobile networks have got their education networks in place such as the GSMA Fraud Forum, but many MVNOs are outside that information loop. So they are hiring guys like me to come in and do fraud reviews to bring them up on industry best practices.



What are these MVNOs doing wrong?

They basically don't understand the fundamentals of fraud management. For example, in near real-time roaming data exchange, they often don't look at those records because they don't understand their importance. Many are not even aware that IRSF exists.

Now the 'Light' MVNOs are probably in a bit better shape because their traffic is going through a large network operator who has the necessary fraud defenses in place.

Those 'Full' MVNOs who have their own core network are probably more exposed because most have not implemented any fraud management tools. Then the other thing that works against MVNOs is that their operations are very lean and they make their money on volume and low prices.

Sure, they treat telecoms as a no-risk commodity to offer, like selling cinema or lottery tickets. Some of these MVNOs are grocery store chains.

Yes, most of the emphasis is on acquiring customers. Even if the MVNO appoints someone to be a fraud manager, that function often gets low priority.

They also don't realize that they can get into a fraud management system for a reasonable price these days. Some excellent tools are available that run around $100,000. The days of million dollar fraud systems for small to medium operators are gone. And some of these suppliers are offering 24/7 fraud monitoring via a managed service. The managed service is a good fit for a medium-sized MVNO because it's not efficient for them to employ dedicated people to look at fraud records.

So what do you prescribe for these MVNO organizations? What do you consider they need to do?

Well, I think the actions they need to take generally boil down to five steps:

1. **Fix accountability** — Assign someone in the organization to be responsible for fraud management. They may not be big enough to appoint a full-time fraud manager, but someone needs to be accountable. At some MVNOs whoever answers an incoming call about a fraud issue is responsible for handling it. That sort of policy is too loose and doesn't take the risk seriously. Your average person has no idea how fraud occurs.
2. **Make an investment in training** — Whoever is appointed to the job needs to spend some time learning the basic principles of fraud management, at least. They must learn what's required to bring their organization in line with industry best practices for their smaller shop. Because people don't have the background in fraud, they end up being purely reactive. A solid fraud program needs to be proactive — and it's best to develop a two or three year strategy for implementing programs they need to build.
3. **Invest in Automated Tools.** — It's not practical for MVNOs to put people behind a desk 24/7. They have got to look at an inexpensive and automated fraud management system with the ability to send an email or text message to alert someone when the system identifies likely fraud. About 90% of all IRSF happens between Friday night and Monday morning. No one in the organization is working during that period so you must cover that period with an automated system.
4. **Do a Full Risk Assessment**-- It's worth having someone like me come in and do a fraud health check to see where their risks are and what controls should be in

place. In every fraud risk audit I've done, the organization was surprised at the level of risks they were exposed to. CFOs are giving fraud management a low priority, but that's because they don't understand the risks. Actually the damage could be anything from $1,000 a week to $500,000 a week.

5. **Enlist the Aid of the MNO Supporting Them** — Another key thing is to look over their agreements with their MNO supplier. One of the surprises is the contracts in many cases date back before the time when IRSF was an issue, so fraud management doesn't even appear as a line item.

   While an MVNO is expected to manage its own fraud risk as far as acquiring customers and offering products and services, it's important that the MNO agrees to remove their margin in IRSF rather than profiting from it. The MNO should at least be stopping the fraud once it's detected to minimize the damage.

Colin, when you go in and consult with an MVNO, what's the typical procedure?

When I do get called in to consult, I get all the information I can about the organization — who they are, customers, and products and services. Then, over a 5 to 7 day period, I'll typically interview all of the execs from the CEO on down and any Key Stakeholders in the next level of management.

With that information I'll have a better understanding of their products and services. If they've suffered a fraud loss in the last year, I'll review each fraud case and identify every point of failure that contributed to that fraud.

From there, I start compiling a complete risk profile for the organization, what controls are missing, and what opportunities there are. Typically I'll come out with 15 to 40 recommendations on where to protect their network.

So usually within 2 week's elapsed time, they come away with a complete framework for what they need to do. And I also leave them with documented policies and instructions as well.

Sounds like a must-have audit for an MVNO. Thank you, Colin.