The Black Swan Series of Telecom Solution Guides

The Value of an Authoritative Database of Global Telephone Numbers in Fraud Blocking & Business Analytics

Expert Commentary by

John Haraburda, Principal Solutions Engineer Director at iconectiv

Drawing on the Experience of Serving 50+ Clients at

Tier 1 and Tier 2 Carriers & MSOs in North America, Europe & Africa

Who Subscribe to & Use the

TruNumber Protect Database

Table of Contents

A. Black Swan Editor's Introduction

Dear Colleague:

What if a Fraud Management System came along that could automatically detect and block 90% of IRSF and Wangiri fraud cases coming through your network – and even make accurate blocking decisions on numbers never-before-seen?

Think how productive that FMS could make your fraud analyst team. With most fraud attempts quickly blocked, analysts would have more time to track down the 10% of tough or usual cases that require their expert attention.

Well, such a system exists, but it's not really an FMS. Actually it's a database designed to work in tandem with an FMS. And it enhances the value of any FMS or fraud-fighting team that takes advantage of its intelligence.

I'm referring to iconectiv's TruNumber Protect, an authoritative database of allocated numbers and special number ranges in every country of the world. The database has proved its value for over a decade and is now in use at 50+ carriers. In fact, many Tier 1 carriers around the globe, such as British Telecom / Everything Everywhere, Deutsche Telecom Group and Verizon, have made TruNumber Protect integral to their fraud control program.

I've heard about iconectiv's database for years, and assumed it was a supplementary solution tailored to the needs of large carriers.

But having discussed TruNumber Protect in great depth with iconectiv's principal solution engineer John Haraburda, I now view TruNumber Protect as an invaluable **pre-FMS firewall for blocking fraud** even before the call goes into signaling.

And while large carriers are indeed the biggest financial supporters of TruNumber Protect, iconectiv also sells the solution to many mid-sized carriers who pay based on their traffic volumes.

Analytics and the Law of the Hammer

Many of you have heard of the Law of the Hammer which states:

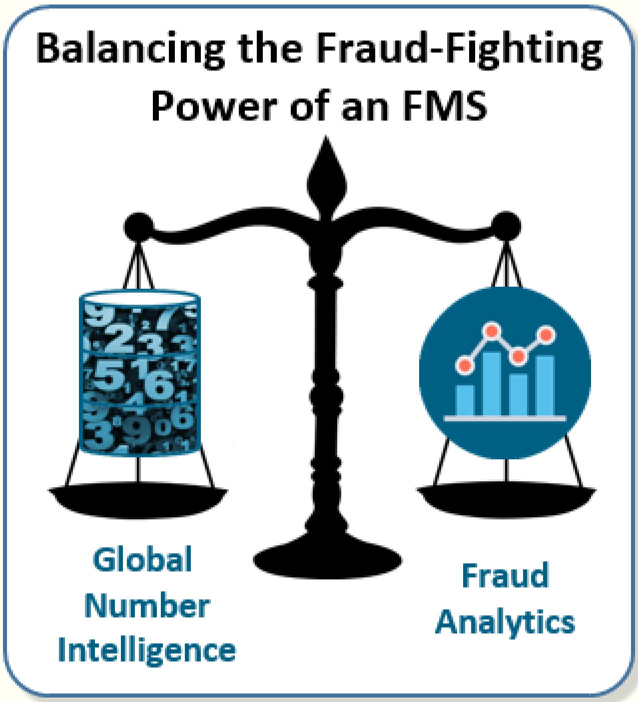
> "If the only tool you have is a hammer, you tend to treat every problem as if it were a nail."

Well, in the telecom fraud-fighting game, the hammer is analytics. Analytics – and its machine learning and AI cousins – are what you throw at almost every fraud problem.

Historical user profiles, blacklists, and keeping call statistics all involve cranking the analytics engine.

But TruNumber Protect tackles the same fraud detection problem in a simpler way: it instantly identifies 90% or more of live fraud threats without performing a single FMS calculation or analysis.

So TruNumber Protect is a very different kind of tool. It's embedded intelligence, a kind of gold database whose power is **not** based on tracking past fraud cases, but on its ability to assess the legitimacy of every single voice call dialed or SMS sent.



In this role, TruNumber Protect fills a vital intelligence gap. For decades, fraudsters have exploited the fact that tens of thousands of carriers and MVNOs around the world really don't know which international phone numbers are real and which are fake.

The fraudsters are adept at exploiting unallocated numbers or special-purpose numbers for their criminal purposes.

But with TruNumber Protect's database integrated into your switch routing engines, you can easily separate the wheat from the chaff.

In short, fraud managers need to better balance the use of number intelligence and analytics in their fraud-fighting strategies.

The Investment Required to Maintain a Global Number Database

Significant on-going investment is required to maintain an authoritative database of this type.

By analogy, think of an international GPS system that maps the world's vehicular highways and roads.

Keeping such a GPS system accurate is a never-ending process because new road construction and the buildout of towns and cities constantly alter the global map. And in the equatorial countries of South America, Africa and Southeast Asia, thick vegetation hides the roads from even satellite view. Ultimately, every global GPS system maker is forced to put feet on the ground – to hire people around the world to do the painstaking research – and maintain contact with key data sources.

The same goes for iconectiv's global numbers database. The allocation of number ranges is in constant flux and it's costly to develop and maintain personal relationships with regulators in all countries large and small. Great care and thoroughness is required to keep the database truly authoritative.

Very few organizations are skilled in that, but iconectiv has created an entire business around number intelligence. iconectiv is also the administrator of the NPAC number portability database in the U.S. and at dozens of other countries around the world.

Highlights of this Guide

John Haraburda does an excellent job of sorting out the details behind TruNumber Protect in this Guide. Here's a preview of key things you'll learn in the Guide:

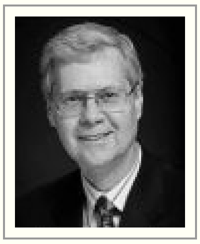
- **TruNumber Protect Flexibly Integrates with Your Fraud System.** Management of your custom fraud control preferences is done through the TruNumber Protect on-line portal which enables flexible rules setting. The rules stay consistent even when the database is updated. In fact, you can even build rules upon rules.

- **Best Practices in Leveraging Numbers Lists** -- John walks through the use of numbers intelligence and shows the pitfalls of being too-reliant on industry- and vendor-blacklists. He explains how the fraudster preference towards higher-volume and lower-tariff campaigns will require rethinking fraud detection methods.

- **Fraud Analyst Productivity Benefits** – While blocking fraud loss is the biggest benefit of using TruNumber Protect, John explains the substantial staff productivity gains that result from using TruNumber Protect pre-FMS blocking of fraud.

- **Employing the Database in Other Use Cases** – John supplies interesting examples of how analytics can leverage TruNumber Protect to create valuable insights. Plus, carriers who subscribe to TruNumber Protect regularly use it in areas such as billing, least cost routing, SMS revenue assurance, and profit margin analysis.

In short, the Guide will give you a great appreciation for how an authoritative global database of phone numbers may benefit your fraud control operation.



Dan Baker, Research Director of TRI
Editor, Black Swan Telecom Journal

B. An Authoritative Database of Global Numbers

1. Proactively Block Risky Traffic: Before CDRs & Before Signaling

Every carrier has anti-fraud measures in place. The problem is: most solutions are reactive and are not based on authoritative industry intelligence.

A Call Detail Record (CDR) FMS raises alarm and detect frauds after the fact. Modern signaling-based FMSs (Mobileum, Subex, Oculeus, TransNexus) can block calls before the call is connected, but cannot handle a zero-day attack because the fraud blocking is based on blacklists or machine learning, which relies on historical analysis.

iconectiv's TruNumber Protect database is different, its authoritative industry intelligence tells when a call is a fraud risk by the active status of the international number being calls. In fact, TruNumber Protect can block calls before they even go into signaling. It works with the least cost routing system on the switch. And that routing engine will generally be set to do one of two things: block the call outright or push the call to a voice mail.

The cloud environment creates customized feeds for the routing system. Data is then pushed into those systems, and those systems don't need to ping TruNumber Protect.

In short, the interexchange carriers, the SMS gateways, are all protected. TruNumber Protect is used to either: 1) proactively block the call so the fraud never happens or 2) allow the call to go through but escalate the alerting of it in your fraud management system.

2. Key Benefits of Using an Authoritative Numbers Database

The value of TruNumber Protect's authoritative, pre-call blocking can sometimes be extraordinary.

One carrier customer had a Wangiri attack hitting 600,000 customers but it had zero fraud impact because the carrier proactively blocked the traffic with TruNumber Protect. Just knowing those 600,000 customer attacks were being sent to unallocated numbers identified them as risky – and every one was blocked automatically.

Here are the key benefits of TruNumber Protect:

- **The Value of the FMS is Greatly Enhanced** -- By leveraging the automation and integration of TruNumber Protect into the various carrier system/platforms, you're now able to optimize the performance of the systems you already have.

  The deep telecom number intelligence inside the TruNumber Protect database enhances the value of every FMS that accesses it. Every switch can have a barring list of traffic you automatically want to block. And the intelligence is available to switch routing engines as well as SMSC gateways.

- **Boosts Fraud Staff Productivity** – The fraud control richness of the TruNumber Protect data will take a huge workload off the fraud department staff. By reliably identifying and proactively blocking 90% of the fraudulent call attempts, the staff can spend more time working on the 10% that require deeper investigation.

  A company might have 200 to 500 fraud alerts a day – maybe too many for the fraud team to adequately screen. In other words, the intelligence TruNumber Protect provides increases the value of each fraud professional to the company.

- **Protects the Customer's Trust** – By blocking fraud proactively, you not only stop the fraud from happening but also stop all those tickets going to the customer care desk. You stop billing the customer for bad usage. And you improve the customer experience. Result? ARPU is maintained and churn is minimized.

- **Boosts the Power of Any System that Benefits from International Phone Number and Carrier Intelligence** -- Business intelligence (BI) can tap into this intelligence for hundreds of use cases the carrier conceives to aggregate and correlate the data to provide better intelligence or more nuance/color to operations.

C. The Power of Global Number Range Intelligence

1. An Authoritative Source for Unallocated and Special Numbers

FMS vendors and other solution vendors provide blacklists of numbers associated with past fraud. In fact, one of the major fraud forums publishes a list of fraud alerts to their membership on a regular basis.

Recently, iconectiv took a month of alerts from that blacklist and found that 92% of those alerts we already identified as fraud risky in the TruNumber Protect database. TruNumber Protect's catches far more fraud because it includes information on every number range for every service type and every carrier in every country in the world. That gives customers the ability to really understand their risk profile and determine whether or not they want a call to happen or not.

Unallocated numbers are the number plans controlled by the national regulator that are not associated with a carrier. For example, across the Atlanta metropolitan region, the regulator controls many number ranges that are not yet assigned to a carrier. The allocated numbers in the Atlanta area are those assigned to AT&T, Comcast, and other carriers active in the region.

So technically, when there's no switch at the far end to receive the call, any call to that number plan is illegitimate. And when a phone call is made to a number that doesn't officially exist – those are the unallocated number ranges that fraudsters try to exploit.

Now, within the allocated ranges there are also special number ranges, such as numbers used for paging devices. These are also risky numbers, especially if you see paging numbers having 300,000 minutes of use and an 8-minute average call duration.

But once again, TruNumber Protect identifies that upfront. It's the authoritative source of risky numbers. And the database is bigger, broader, and more precise than anything competitors offer.

1. How are Unallocated and Special Number Ranges Obtained?

iconectiv has been working with national regulators for decades. iconectiv is the administrator of the NPAC number porting clearinghouse in the U.S. market and is the administrator for number porting clearinghouses for many other countries around the world.

The key advantage is the information is authoritative: it's coming from the authoritative sources including the country regulators and authoritative carriers. It was not assembled by tapping into an HLR or any third-party data sources.

2. Why You Need Intelligence on Unallocated and Special Number Ranges

The usefulness of TruNumber Protect's number classifications is that it can more quickly and easily identify International Revenue Share (IRSF) and Wangiri frauds than any other solution. Here's a rundown of what it does:

- **The Number Hijacking IRSF** (or short stopping fraud) is where the call is redirected by a carrier in the billing stream to terminate in a destination elsewhere in the world. Often the fraud is conducted in partnership with interexchange carriers who are in on the scheme to artificially pump fraud traffic. For example, if you call a phone number with a country code for Cuba, it appears to go to Cuba but, in reality, the call may leave the U.S. carrier's network, goes to an interexchange carrier, but then get redirected to Ecuador, or Botswana, or maybe Indonesia. Eventually, the call terminates but it never got to Cuba.

- **Special number traffic** – [*Premium Chat, Carrier Services, Internet Access lines etc.*] is often allocated to a local tariff plan and billed at local rates within the country. However special numbers are often billed at exorbitantly high termination rates when called from an international number.

  So these numbers are high risk for fraud and traffic pumping because even though it's a legal call, it's meant to generate usage at a high termination cost.

  Calls are also allocated to information-providers who sometimes use special numbers to commit fraud.

- **High Volume, Low Tariff Fraud** -- Setting calling volume and monetary thresholds for detecting fraud is an established fraud control practice. But as fraudster mature in their use of analytics, thresholding becomes a less effective means of detecting them.

  If the carrier starts looking at five calls in the past hour or $25 a fraud, the fraudsters gradually discover what those thresholds are by keeping statistics on the numbers being blocked. So, if the threshold is set at $25 in 24 hours, they'll pump only $23 of fraud a day to that carrier and, therefore, stay under the fraud radar screen.

  While a carrier will notice if they experience a major fraud hit, they don't often notice if it is an on-going low level fraud that adds up over time because the fraudster stayed below the thresholds.

  Once again, since TruNumber Protect keeps track of the unallocated numbers that fraudsters use for high volume/low tariff fraud, it identifies the risk traffic immediately.

In short, the value of TruNumber Protect intelligence is that even if it's the first time you've seen a particular number or number range being called, you already know it's risky.

3. Getting Better Fraud Blocking Results than a Black List

Since TruNumber Protect has been serving carriers for over 10 years now, iconectiv often gets the opportunity to examine a carrier's effectiveness in blocking fraud. For instance, iconectiv is frequently asked to look at three months of usage data to see whether TruNumber

Protect would be a good investment with a strong return on investment (ROI). Often, it is found that there are errors in the in-house barring list that a carrier maintains.

One carrier with a competitive solution to iconectiv's had a custom-created fraud blacklist. The carrier thought they had protection in certain countries. Several months later, however, that proved to be the source of a major fraud hit.

When the company compared their home-grown blacklist to the iconectiv data, they had less than 2% of the numbers that should have been classified as risky on their list. iconectiv's solution would have identified that fraud, which existed through the entire three evaluation time frame.

4. A Better Way to Screen Calls for Fraud and Allow Low-Risk Calls

Hitting the low lying fruit of fraud detection is not going to be effective. You may catch the obvious high tariff destination fraud, but there's plenty of fraud happening these days in low tariff, but high volume attacks that "fly below the radar."

Another problem: carriers are sometimes too eager to block traffic to a specific country when they could be doing good business there in legitimate call revenue. TruNumber Protect solves this over-blocking issue, by giving the carrier comfort in knowing exactly which number ranges in a country are dodgy and which are legit.

In short, TruNumber Protect enables the carrier to make an accurate measure of the risks and open up risky countries to legit business.

D. Enhancing the Power of Your FMS

1. Full Integration with your Fraud Management Systems

TruNumber Protect is platform agnostic. The solution is sold to the carrier and iconectiv ensures TruNumber Protect is integrated into the current (or future) FMS provider.

Today, iconectiv regularly works with and interfaces to fraud detection players like WeDo, HP, Subex and others. So think of iconectiv as enabling the carrier or FMS vendor's solution to become more knowledgeable, efficient and organized. It's all thanks to the constantly refreshed baseline of global telephone number intelligence in TruNumber Protect.

Another advantage: TruNumber Protect does **not** require anything intrusive, such as putting collection points on the SS7 network.

The point is that TruNumber Protect can substantially **upgrade the existing FMS** without you having to go out and spend X million dollars buying a whole new platform.

Even analytics can be integrated into the use of TruNumber Protect.

1. Flexibility in the Way Fraud Blocking Rules are Applied

It's natural to assume that if traffic is risky or dodgy for one carrier, it will be for every carrier. But that's not what iconectiv has seen in actual practice.

iconectiv has seen different carriers using different risk parameters, even in the same country. Carriers vary on what traffic they will allow, and many times their decisions depend on their interconnection tariffs or roaming agreements.

So when you have a fraud solution that says "all these are fraud, block all this traffic" -- that's not always the case.

iconectiv ran into an Asian carrier who uses unallocated number ranges for internal network routing. When iconectiv labeled that traffic as risky, they confirmed it was legitimate saying, “That's the way we do SIP peering to interconnect to different countries in the region.”

So it's valuable to give each carrier the autonomy to control its own fraud rules and exceptions. That flexibility is built into the TruNumber Protect Cloud.

2. How TruNumber Protects Fraud Control Rule Exceptions

A key benefit of the TruNumber Protect cloud is its ability to deliver customizable output formats for each use case you choose to build into your environment.

Your FMS can directly ingest the precise information you need from TruNumber Protect. Not only will it automatically load the updates of the database, it will retain the customized exceptions list you’ve created for your organization. Exceptions are made by merely making changes in the portal.

Carriers will typically load everything in the fraud system that looks risky or dodgy. They will then create a new set of alerts where the traffic coming in hits one of the categories TruNumber Protect is monitoring.

Now, as they use the data and create fraud alerts and process them, they can modify their rules. They might say, "Hmm, this premium traffic to Country A and Country B keeps popping up. It looks really dodgy, so I'm going to add that to our proactive blocking list.”

And to perform that change, they merely go to the portal and change the rule set to create a new output format that automatically moves into the routing system to block that traffic.

However, if next week, if there are requests to call that country in question, you can easily set up a new exception to the rule you created. It will allow certain numbers to be called, but all the other numbers in the range would still be blocked.

So as you can see, rules can be built on top of rules – and the TruNumber Protect portal keeps track of all these exceptions even as new updates are constantly added to the global intelligence TruNumber Protect maintains in the cloud for your daily use.

E. BI/Analytics & Operations Use of TruNumber Protect

Certainly the most common use of TruNumber Protect is to automatically block the unallocated and special numbers uses in frauds such as IRSF and Wangiri.

But above and beyond these uses, TruNumber Protect is a valuable reference database with many BI/analytics and operations uses:

1. Fraud Analytics using TruNumber Protect

Here are some examples of how analytics and the TruNumber Protect database work together:

- **Wangiri Fraud** -- Several customers use TruNumber Protect's intelligence to interrogate the inbound call, the A Number. And with Wangiri attack, you hardly ever have conversation time because the phone rings two times and hangs up.

  However if you know a dodgy A Number is trying to contact users across a wide distribution, you can identify that with TruNumber Protect and create some rules to address it.

- **Group Carrier Flexibility** - A big group telecom like Orange will tend to treat their traffic differently depending on the country OPCO. Likewise, roaming traffic is treated differently than on-net traffic.

  So with TruNumber Protect's on-line portal, they have flexibility to apply the data locally -- to decide what's risky or not from the OPCO's perspective.

- **Follow-Up to a Never-Seen Number** -- What happens if you've never seen a number range in your country before? An AI-based system won't know if it's a risky number or not because there's no history of the number in its learnings.

  However TruNumber Protect will immediately recognize the call as going to an unallocated number in Cuba, so the call is blocked.

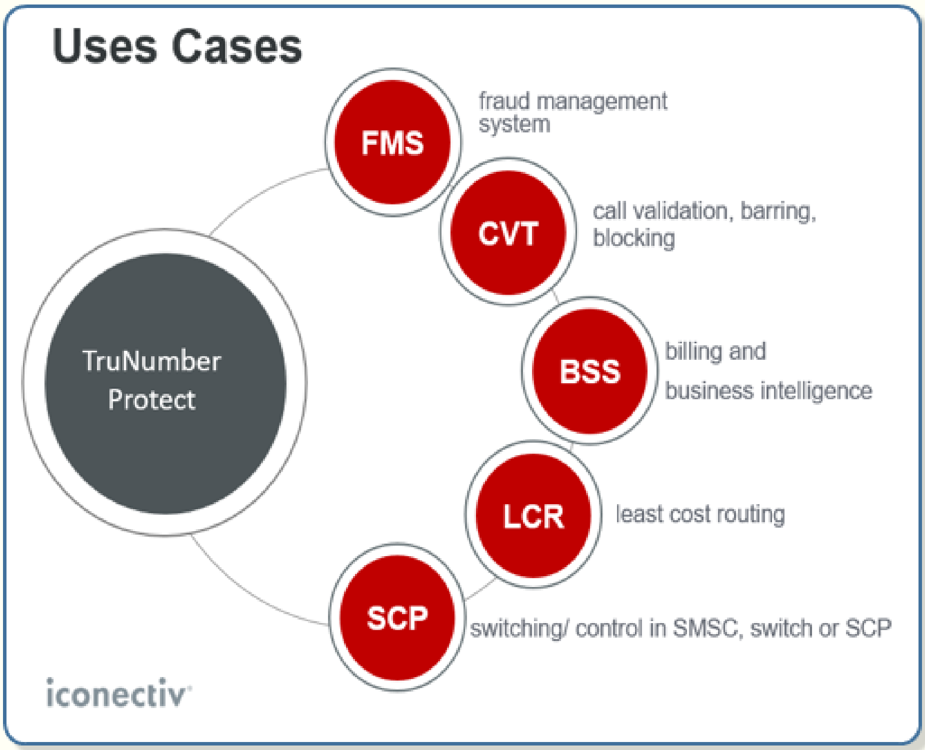
  Where the analytics/AI comes into play is in the follow-up: an email message is sent to the enterprise, saying: "We blocked a highly suspicious call made after working hours today from your Cleveland, Ohio office. Our analysis says that the PBX at your Cleveland branch office may be hacked and compromised. We suggest you change its password immediately."

2. Operations Uses of TruNumber Protect

Another benefit of the TruNumber database is all the supplementary information it gives you. Since TruNumber Protect is an authoritative data source, it allows you expand the granularity of your analysis or aggregation.

For example, TruNumber Protect includes valuable info on the carrier, the type of service, and the category of the service such as satellite number or a premium chat number.

The chart below displays many additional use cases (beyond fraud control) that can be integrated into the platform at no additional cost.



- **Least cost routing** -- Many countries, such as the UK, do not employ a national number portability database. However TruNumber Protect categorizes phone numbers by carriers, so you can determine the numbers associated with three largest mobile carriers in the UK: Vodafone, 3, EE/BT. This is valuable intelligence you can apply to sharpen your least cost routing solution.

- **Billing** – With TruNumber Protect, you can add accurate city, state, and country information on the invoice you send customers.

- **SMS Revenue Leakage --** When an carrier erroneously sends an ASP message out of an SMS gateway toward a non-mobile (fixed) carrier or free (800) phone number, that ASP message will not reach its destination because fixed and free number do not receive SMS. However, you're still billed for every ASP message whether it goes through or not.

  But since TruNumber Protect maintains the service type for every carrier in every country, you can easily determine whether a number is a mobile number or not – so a revenue leak can be closed.

- **Evaluating tariff plans and profit margins** is another popular use for TruNumber Protect whose data is joined with IEC termination prices to optimize price lists. TruNumber Protect geographic location info in Brazil, for example, will enable the carrier to compare traffic flows through Sao Paulo vs. Rio de Janeiro, Brazil's largest cities.

In short, you have full autonomy and flexibility to choose the BI/analytics use cases you use TruNumber Protect for. And we make it easy to integrate that intelligence so you can ingest it into your own in-house or vendor analytics solutions.

F. Buying & Implementation Concerns

1. TruNumber Protect Customers & License Pricing by Carrier Volume

Currently there are 50+ customers of TruNumber Protect across the Americas, Europe, and Africa. Many customers in North America and Europe have been onboard for over 10 years. Of course, carriers of all sizes subscribe to TruNumber Protect, and iconectiv tailors its annual license fee to the volume of traffic the carrier needs to protect.

Large telecom carriers and cable carriers invest in TruNumber Protect because their risks are higher and a large volume of their traffic is international. Routing complexity is another factor that increases the fraud risk. About half our business is being driven by Tier 1 carriers.

In the U.S. market, there are some ~1,600 carriers and probably 80% of them are doing low volumes of international traffic. So, at those carriers, IRSF and Wangiri problems can be monitored more closely because the volumes are lower. However fraud spikes do occur that catch them.

But no matter who the carrier is, iconectiv sees a 3-month ROI with TruNumber Protect – a good return on the investment. And that's only looking at the fraud use case. If the carrier integrates TruNumber Protect with other use cases in margin management, revenue assurance, and network routing, the ROI is often a month or less.

2. Implementation: Getting Started with the Database

When iconectiv first implements the solution at a new customer, they walk them through the functionality of the portal, and cover the nuances and best practices of how to use the data. They also regularly check existing customers to make sure they are getting the full value of the solution set.

Implementation is usually quite rapid. Recently the company did a traffic analysis for a new customer. By the time they got the contract signed and processed, iconectiv was able to stand up the production environment of the portal, give them access to it and train them in the week after signing the contract.

3. Deciding whether TruNumber Protect Fits Your Organization

When iconectiv starts a sales cycle with a new carrier they first perform an analysis on their historical usage over a period of time. They also look at their history and other factors including PBX hacks or voice mail hacks or stolen SIM cards.

iconectiv often takes historical usage for 1 to 3 months, and does an analysis on the usage to see how TruNumber Protect could have impacted and identified risky traffic on the network.

The result of that data analysis then becomes the business case to internally justify purchasing TruNumber Protect.

G. About iconectiv

1. iconectiv and its Track Record in Third Party Telecom Databases

Several customers have told us they trust iconectiv because we've been around for decades as Telcordia and originally Bellcore, the R&D arm of the Regional Bells who were formed in 1984 when the Bell System was broken up.

Today, iconectiv is owned by Ericsson and Francisco Partners. The company operates as an independent company and has its own independent board of managers. And as you'd expect iconectiv is quite active in industry associations such as GSMA, CTIA, and CFCA.

The business of iconectiv is to maintain hard-to-obtain data from regulators and carriers around the world. In addition to maintaining the complex matrix of international number ranges, TruNumber Protect, iconectiv is also the administrator of the NPAC, the number portability plan of the U.S. market and the world leader in numbering solutions.

Now the FMS and analytics solution firms don't do this type work. Managing registry and numbering solutions is iconectiv's core business and the intelligence gathered can add enormous value.

H. iconectiv Literature

"Moments Matter" in Blocking Identity Fraud: Why Number Porting Data is a Vital Tool in Stopping Account Takeovers

I. John Haraburda, iconectiv

John Haraburda, Principal Solutions Engineer Director at iconectiv, is responsible for managing critical business operations and spearheading business development to help customers solve real world problems.

John supports the iconectiv TruNumber Protect and Routing solutions which bring network and margin optimization to carriers around the world. By proactively addressing traffic in the carrier network, iconectiv enables our customers to mitigate risk for fraud; maximize their margins and efficiencies; and optimize the performance of existing staff and systems.

John has extensive experience in bringing revenue assurance and fraud solutions to the global market. Prior to iconectiv, John served in roles as Product Line Management and Solutions Engineering; Head of Revenue Assurance and Fraud; and management positions in billing, program management and finance.

John holds a Master of Business in International Business from American University and a Bachelor of Arts from George Mason University.

J. The Black Swan Series of Telecom Solution Guides

The Black Swan Series of Telecom Solution Guides are deep dive one-vendor-specific papers that focus on one Solution category. These objectively written papers under TRI's editorial and industry analyst guidance feature the commentary of solution vendor experts.

Each **Solution Guide** educates telecom professionals and solution buyers on a Solution's important features and benefits. Tailored to the uniqueness of each Solution, the **Guide** may cover any number of topics from industry trends driving need for the solution… to mini-case studies, best practices, and advice around buying, implementing, and using the Solution.

If you are a Solution Vendor interested in having a Guide prepared for your organization's solution, please email TRI to receive a detailed proposal and order form.

K. Technology Research Institute (TRI)

Technology Research Institute (TRI) has been writing and researching telecom software and systems markets since 1994. Its industry reports have covered the gamut of telecom systems from billing and service assurance... to customer care and provisioning.

In recent years, TRI's research director and owner, Dan Baker, has authored major reports on Fraud Management, Business & Revenue Assurance, Telecom Wholesale Solutions, and Telecom Analytics/Big Data.

And since 2011, TRI's on-line magazine, Black Swan Telecom Journal, has covered issues of the day in telecom fraud management, revenue assurance, analytics, IoT, operational excellence, and optimization.-

