

FRAUD MANAGEMENT IN AN ITSP ENVIRONMENT

Boaz Bechar

Humbug Telecom Labs, Ltd.

July, 2011



ABOUT THE AUTHOR

Boaz Bechar is an entrepreneur in the telecom industry and cofounder of Humbug Telecom Labs, a company serving organizations of all sizes, offering carrier-class telecom analytics and fraud prevention tools. Previously Boaz cofounded an Internet Telephony Service Provider (ITSP) serving millions of users worldwide, and operating in partnership with global brands. Mr. Bechar has years of hands-on technical experience in management, development and deployment of telecom and billing applications from the ground up.

1. BACKGROUND

In the early 60's John "CrunchMan" Draper used a whistle found as a prize in a Captain Crunch cereal box in order to exploit AT&T's network, then based on in-band signaling. Blowing 2600hz tones into the phone's handset, CrunchMan was able to bypass the carriers billing systems and place free international calls, bringing him to celebrity status among hackers, and sling-shotting telephony security to the limelight. In the years that followed, the telephony security sub-culture would revolve primarily around various 'colored boxes' (blue box, black box, red box, etc) each with different capabilities to generate different tones, exploiting various features and vulnerabilities within the telephony network.

Technologies have evolved since CrunchMan's hacking days, and with them, hackers and their sophistication, techniques, and motivations. To make things more challenging, the rapid adoption of IP-based telephony technology by businesses and consumers, has opened up telephony security to a wider spectrum of security enthusiasts, who have readily available information, resources, and computing power to rapidly cover and probe networks at a global level.

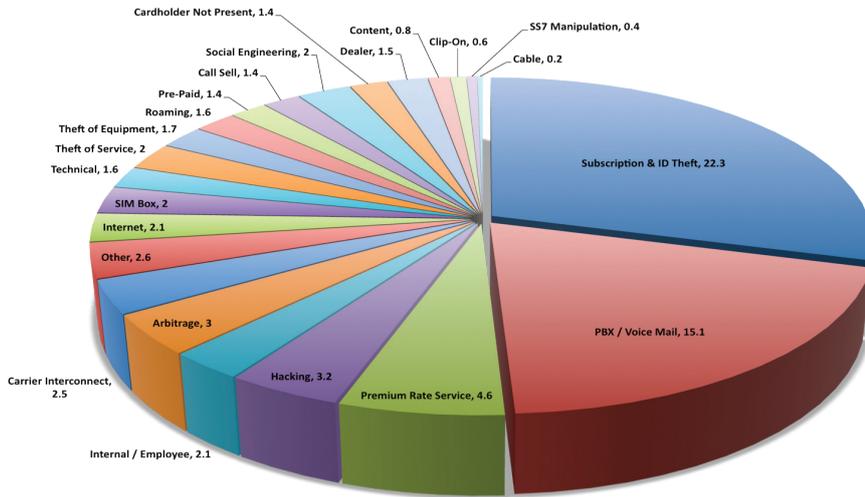
According to the Communications Fraud Control association 2009 Global Fraud Loss Survey, over \$80 billion are lost each year to telephony fraud, with the top three predominant sources being Subscription Fraud (\$22bln), PBX/Voicemail Hacking (\$15.1bln), and Premium Rate Service Fraud (\$4.6bln). According to the survey, 91% of participants felt that global fraud losses had increased or stayed the same, while 78% said fraud has trended upwards within their company.

Most notably however, the CFCA survey reveals that carriers suffer between 1 and 4.5% in fraud losses from their total annual revenue – a serious issue for management to tackle. To combat this, carriers employ dedicated fraud management teams and have revenue assurance procedures intimately connected to all aspects of the organization, from accounting and operations to technology.

Over the last decade, internet-based telephony has exploded in popularity and allowed new services and service providers to emerge with low barriers to entry and minimal setup and infrastructure costs - an environment which tends to dangerously underestimate the need for investment in revenue assurance procedures. As with any traditional telecom operator, ITSPs suffer from constant fraud attacks and revenue leaks, and depending on size, user base, and growth, fraud can either be constant or a come-and-go problem.



Bluebox by Steve Wozniak in the Computer History Museum



2. THE ITSP ENVIRONMENT

The resources at the disposal of most ITSPs pale in comparison to long-standing telecommunication companies with last-mile infrastructure, however in some cases this can play to the advantage of the ITSP - enabling it to capture niche markets, win customers through product innovation, as well as compete on price margins, with low operational overheads to cover. However, while resources are expended on product development, customer acquisition, and even infrastructure expansion – revenue assurance procedures tend to be implemented soon (if not minutes) after an attack has been discovered.

With consumer-focused ITSPs the variety of services and features offered to the user are abundant. Packaged in complex destination-based service offerings, with monthly or pay-as-you-go packages, an ITSP, on the face of it, has the same level of service-sophistication (if not more) than traditional carriers. Behind the scenes, however, ITSPs are lagging far behind in their ability to handle cases of fraud due to a lack of investment in fraud prevention and a rather reactive approach to revenue assurance.

The ITSP perhaps is not entirely at fault, as in-house revenue assurance knowledge and fraud prevention technologies employed by carriers are fiscally unfeasible for the operational model and margins which most ITSPs work by. This creates an extremely fragmented security environment, with each ITSP left alone to re-discover known prevention strategies, and implement security measures in-house on a case-by-case basis.

For consumer-facing ITSPs, in-house fraud prevention can be a challenging and time consuming task. With product-innovation at the forefront, ITSPs are

racing to release innovative features, which are often challenged for security issues during the quality-assurance (QA) process. While this may be sufficient at first, periods of growth and wide-exposure can lead to an increase in the likelihood of a vulnerability being exposed, as is natural with most cycles of software development (and even more-so in a 'release-and-iterate' environment where features are demanded quickly).

SUBSCRIPTION FRAUD

Consumer-facing ITSPs are battling to optimize their user-acquisition costs versus lifetime value – and are constantly trying out new techniques for signing up users. Registration form fields are reduced, making it as simple as possible for newcomers to join the service, while leaving the ITSP with many questions on who the user is – which may be a challenge when tackling subscription fraud.

In many cases, a free call or free calling credit is offered before/after account creation, allowing the user to familiarize with the system. The revenue-assurance decision tree from here can only get longer and wider, for example: If providing the user with a free call after signing up, what stops them from creating multiple accounts and making multiple free calls?

The low-hanging fruit would clearly be to place limits on the IP address and phone number the user is dialing from/to, however this can get problematic if disposable phone numbers are brought into the equation, and even more-so with hackers who have full number-ranges in their war chest. There is no easy way to tackle this problem – but taking steps to greatly limit the financial exposure can be taken, such as limiting the total calls on a per-destination level, routing all free calls through cost-limited trunks, as well as carefully scrutinizing daily cost, duration and call volume user leader-boards, to make sure they are consistent with your rule-set. Additionally, maintaining blacklists of numbers and registration domains (ie blocking sites such as 10minutemail.com from registering) increases the barriers for fake-subscriptions while not effecting valued users.

Paying users, while the bread and butter of the ITSP, can also be a great concern in terms of subscription fraud. While pay-as-you go based programs do have a certain limit on the financial exposure per user, margins can easily diminish due to costs associated with credit card charge-back fees from accounts

using stolen credit cards or hacked online payment accounts (paypal, etc). Scrutinizing paying users becomes even more critical with postpaid accounts, which may bypass initial checks as a seeming legitimate business, but then the account is used for fraud with no intent to pay (NITP).

To minimize exposure to fraud from paying users, it's important that an 'activation process' take place, where payment details are matched against the users registration data. Other vital indicators become relevant on a case-by-case basis, including review of the users credentials, looking for similar registered accounts, similar billing details previously used on the system, etc.

While ITSPs don't currently have the sophistication level of traditional carrier subscription fraud prevention techniques, they do have the ability to leverage new sets of data unique to their environment, in order to create new activation funnels. One proven technique is matching the password-hash used during registration, against a blacklist of known unwanted passwords as well as against previously flagged accounts. Creating more opportunities for unique data sets and matching against historical information is one method that can easily be deployed in an ITSP environment.

Relying on rule-based results completely can be ineffective and its important to have mechanisms in place which allow anomalies to be spotted. For example, a South-American ITSP serving Brazil may find it an anomaly to receive a transaction from an account with a billing address in Congo. Different techniques work well in different operational scales and requirements, and it's up to the ITSP to find the balance between financial risk and rules required to activate an account prior to manual checks.

SERVICE & APPLICATION LEVEL FRAUD

ITSPs are constantly innovating the telephony marketplace, releasing new services and applications on various platforms, and it can be challenging to continue and maintain, administer and implement new revenue assurance techniques. From online and mobile applications to calling-cards and dial-in services, ITSPs have many gates to watch, and to add to the complexity of the matter, each service may have its own set of security rules. For example, a

web-based calling application may want to limit the amount of simultaneous calls an account may place, while this limit might need to be increased for a multi-line office using SIP connectivity.

Marketing efforts often require complex and dynamic pricing schemes and bundled packages to be offered to users, having direct implications on the accounting and billing systems. Revenue-assurance should play a central role in creating and shaping the available offers, which if left unmanaged, can create fraud and abuse vulnerabilities. For example, calls to low-cost termination points such as the US and Canada are often offered as free destinations, and as such require additional sets of rules in order to avoid exploitation. Limitations on the total duration and call quantities an account can place per destination, time period, as well as setting duration limits on a per-call basis, are all basic steps which can help avoid abuse. Additionally, the implications of subscription fraud can fuel exploitation of calling-plans, through multiple subscriptions of a user maximizing usage to uncharged destinations. Avoiding this is in most cases straightforward, by placing time-based limitations on originating/terminating phone numbers, or depending on the scale of the ITSP, limitations on the first 6-7 digits of the number in order to secure against banks of number-ranges being used.

Although internet based, ITSPs also provide a wide spectrum of traditional telephony services, including IVRs, dial-in services such as DISA/calling cards, and voicemail capabilities. Each application, capability and feature can potentially become a source for fraud, and should be included in all revenue-assurance considerations. For example, given that a hacker can find or break a users voicemail password (typically 4 digits, i.e. 1111), they can call-in to a voicemail system to remotely check the users messages. While not a revenue assurance problem at first, this can quickly turn into a costly attack if the voicemail system has the capability to "call back the user who left this message". Essentially this causes the attacker to make use of the voicemail system to place calls to a premium number under their control, gaining them revenue for each minute they hold the line.

Traditionally ITSPs take a network-security approach to preventing telecom fraud (ie. IP blacklists, firewalls, etc), when in fact this should be considered the last line of defense. Once breached, the internal network of the ITSP is

compromised, and the aftermath can be catastrophic, leading to hundreds of thousands of dollars in financial exposure over the course of mere hours. Without the luxury of traffic monitoring by a dedicated network-operation-center (NOC), weekends and holidays can become a particular soft-spot for hacking and fraud attempts.

LOOKING FORWARD

While ITSPs are moving forward quickly with product and service sophistication, there is still a gap between the operational capabilities of an ITSP to prevent fraud when compared to the incumbent traditional telephony operators. Additionally, while both face the constant threat and need to manage fraud, ITSPs face issues both in terms of implementation abilities and financial capabilities for acquisition and management of prevention technologies. Investment in in-house development of revenue assurance techniques can be challenging, and often times defocussing from immediate targets set by sales and marketing timelines. Furthermore, additional rule-sets and revenue assurance procedures can have complex operational implications, requiring training of support and administrative staff, and constant management, QA, and fine-tuning.

ITSPs will need to continue to be as innovative in seeking new methodologies to prevent fraud as they have been innovative with creating new services and features- and by leveraging the capabilities which online-enviroments create, ITSPs will be able to better secure their networks and revenues. While many ITSPs may struggle to battle this growing threat on their own, many are beginning to collaborate and consolidate information in order to proactively and responsibly manage the problem.

Visit us at: www.humbuglabs.org
Contact us: sales@humbuglabs.org