TransNexus®

TELECOM FRAUD CALL SCENARIOS

Contents

Introduction to Telecom Fraud

According to the Federal Trade Commission, telecom fraud accounted for 34% of fraud complaints in 2012, up from 20% in 2010. These numbers continue to grow, as new technology has led to an onslaught of new telecom fraud tactics. The latest schemes are difficult to track and investigate because of their frequency, their layers of anonymity, and their global nature.

This guide will help you learn about the different types of telecom fraud and industry best practices for detection and prevention.

Three Major Categories of Telecom Fraud

We will divide the many telecom fraud schemes into three broad categories, based on who the fraudsters are targeting. These categories are:

- **Traffic Pumping Schemes** – These schemes use "access stimulation" techniques to boost traffic to a high cost destination, which then shares the revenue with the fraudster.
- **Schemes to Defraud Telecom Service Providers** - These schemes are the most complicated, and exploit telecom service providers using SIP trunking, regulatory loopholes, and more.
- **Schemes Conducted Over the Telephone** - Also known as "Phone Fraud," this category covers all types of general fraud that are perpetrated over the telephone

Premium Rate Numbers

Many of the call scenarios featured in this report make use of premium rate numbers. These premium rate numbers are usually to a high cost destination. The owner of the number will offer to share the revenue generated from calls to these numbers with anyone who sends them traffic. This means that a fraudster who generates bogus or stimulated traffic to that destination will receive a kickback for each completed call.

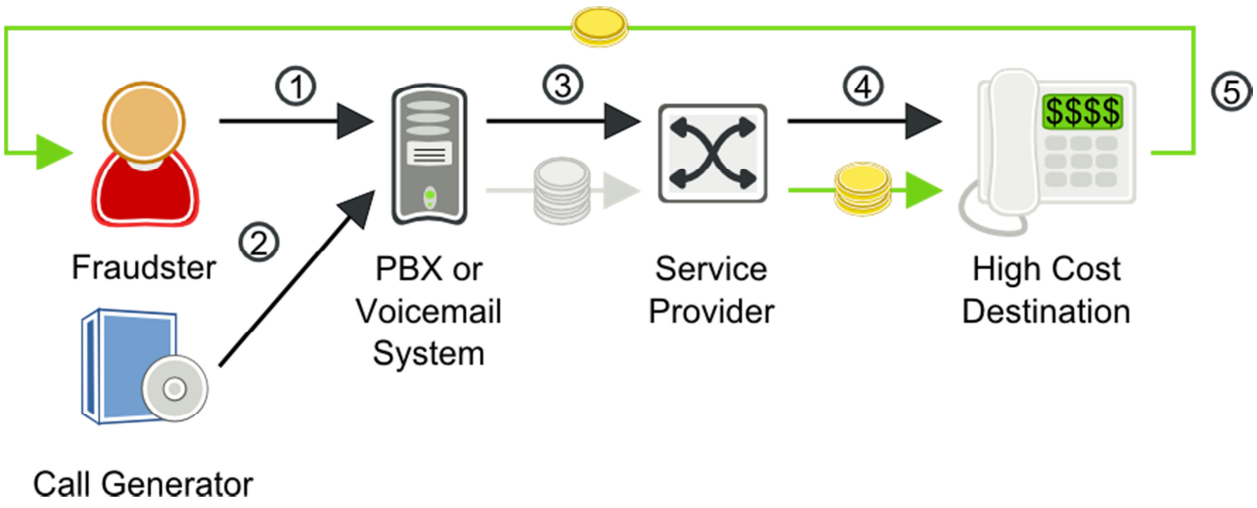
Traffic Pumping Schemes

The first major category of schemes of telecom fraud is called traffic pumping or access stimulation. These are revenue sharing schemes, characterized by fraudsters whom greatly increase traffic to a specific high cost destination. The destination then shares a portion of their profits with the fraudster. The call signature for these types of scenarios are spikes in traffic to high cost destinations.

Fraudsters often take advantage of lax security practices of a service provider's customers. A customer whose network has been compromised will often refuse to pay large fraudulent charges, leaving the service provider to cover the bill. Attacks frequently happen over holidays and weekends, when networks are often monitored less closely.

Call Forwarding Fraud

The Call Forwarding hack is a common form of VoIP telecom fraud. In this case, fraudsters gain access to an enterprise PBX or the IVR of a voice mail system. They can then configure call forwarding to an expensive long distance destination to profit from a revenue sharing deal. Typically the service provider's terms of service clearly state that the customer is liable for fraudulent calls generated from their phone system. In reality, however, few customers ever pay for fraudulent calls and the service provider bears the financial loss because their carrier forces them to pay for fraudulent calls.



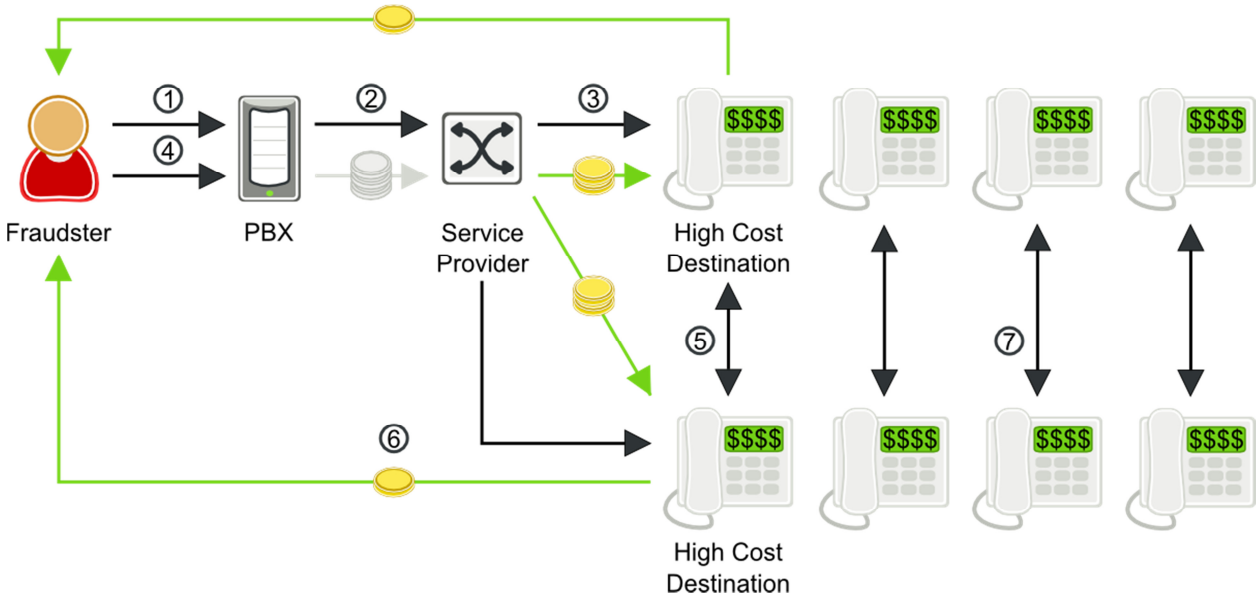
Step	Call Flow	Money Flow
1	Fraudster accesses a PBX or the IVR of a voice mail system, compromises a user's login credentials, and sets the user's account to forward calls to a high cost destination.	
2	Fraudster calls the compromised number over either PSTN or VoIP.	
3	The compromised PBX forwards the call to the service provider's softswitch.	The hacked enterprise technically owes the service provider payment for these calls, but will rarely pay.
4	The service provider switch routes the call to the high cost destination.	The service provider must pay its carrier for the fraudulent, high cost calls.
5		The fraudster has a revenue sharing deal with the high cost destination and receives payment.

Multiple Transfer Fraud

Multiple transfer fraud is an enhanced version of the previously described call forwarding fraud. In this fraud scenario, the call is transferred from the call source immediately after the destination answers the call. When the call is transferred, the fraudulent call is in progress with two high cost destinations and the call source hangs up. This fraud technique is especially harmful for several reasons.

1. Each fraudulent call results in two call legs to high cost destinations.
2. Since the call source is no longer in the call, it becomes more difficult to identify the source of the fraudulent calls.
3. The hacked call source can repeat the process rapidly, one call at a time, to setup thousands of concurrent fraudulent calls through the service provider's softswitch. Most softswitches limit the maximum number of concurrent calls from a single customer. However, this call transfer fraud technique cannot be controlled by concurrent call limits since the call leg from the hacked phone source and the softswitch is very brief. A hacked customer phone with only a single call channel to a softswitch can generate thousands of concurrent fraudulent calls.

Call transfer is a sophisticated technique for multiplying the effects of telecom fraud, while making the fraud more difficult to detect. Once fraudulent calls are transferred, they stay up until the carrier shuts it down. TransNexus customers report calls staying up for over 24 hours.

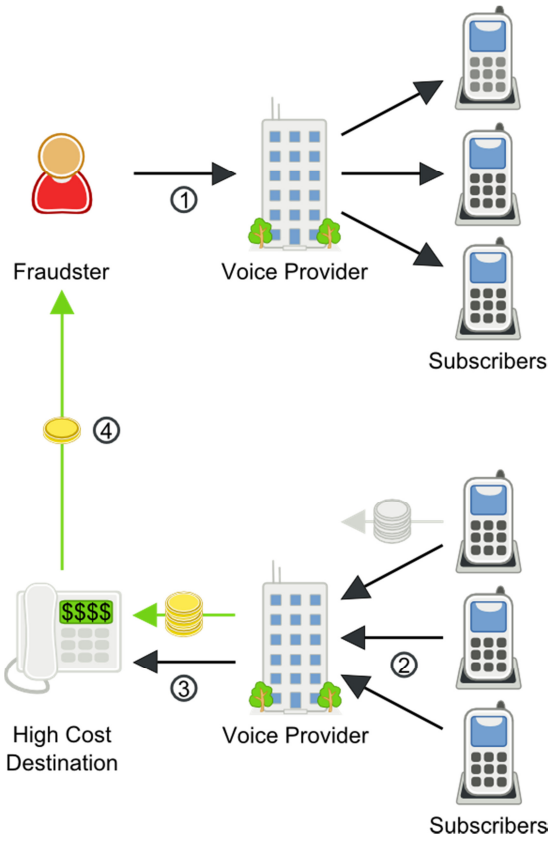


Step	Call Flow	Money Flow
1	Fraudster hacks an enterprise PBX to make calls to high cost destinations.	
2	Compromised PBX sends SIP INVITE to service provider's softswitch.	The hacked enterprise technically owes the service provider payment for these calls, but will rarely pay.
3	Service provider routes call to high cost destination.	The service provider must pay to complete the fraudulent, high cost calls.

4	Fraudster instructs PBX to transfer call to another high cost destination.	The hacked enterprise technically owes the service provider payment for these calls, but will rarely pay.
5	The fraudster hangs up. The call between the two high cost destinations remains in place.	The service provider must now pay for two outbound calls to the high cost destinations.
6		The fraudster has a revenue sharing deal with the high cost destinations and receives payment.
7	Fraudster repeats steps 2-6 to set up hundreds or thousands of simultaneous calls.	

One Ring and Cut (Wangiri) Fraud

Wangiri, in Japanese, means "one and cut." That is, one ring and a cut off phone call. A wangiri phone fraud scheme relies on this single ring method for a quick way to make money. A fraudster will set up a computer to dial a large number of phone numbers at random. Each rings just once, then hangs up. This leaves a number as a missed call on the recipients' phone. Users often see the missed call and believe a legitimate call was cut off, or are simply curious as to who called, so they dial the missed number. This scam is often used to generate calls to Caribbean countries that have the same dial pattern as calls to USA numbers. The number turns out to be a premium rate number – anything from advertising to "free prizes" to sex services.



Step	Call Flow	Money Flow
1	The fraudster sets up calls to voice subscribers, but hangs up after one ring.	Because the calls are not answered, the fraudster isn't charged for making the calls.
2	Curious subscribers see a missed call on their phones, and return the call, not realizing that the number is actually a high cost destination.	The subscribers technically owe the voice provider payment for these long distance calls, but will not be happy to pay, as the number looked like a domestic number.
3	Service provider routes call to high cost destination.	The service provider must pay to complete the fraudulent, high cost calls.
4		The fraudster has a revenue sharing deal with the high cost destinations and receives payment.

Schemes to Defraud Telecom Service Providers

Telecom Service Providers are particularly vulnerable to telecom fraud. Fraudsters are able to manipulate telecom regulatory systems to their advantage, and to the disadvantage of the service provider, in ways that are difficult to detect, trace, and prosecute.

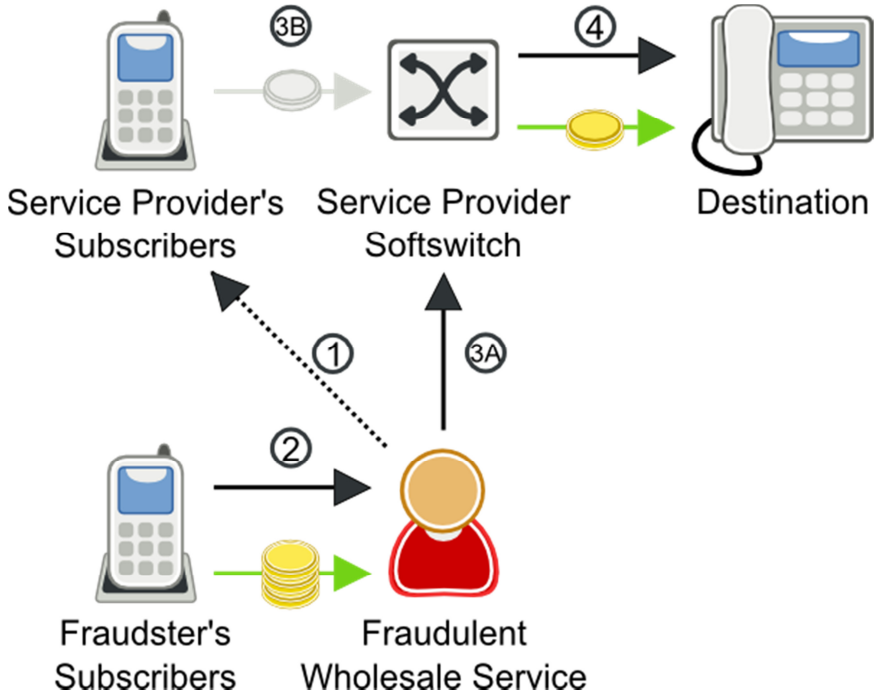
Wholesale SIP Trunking Fraud

Fraudulent wholesale trunking is a relatively new phenomenon, but one that is growing in popularity and difficult to detect. In this scenario, the fraudster is actually making money by selling wholesale trunking services, using stolen credentials to terminate the calls.

The key calling signature for this type of fraud is an increased number of apparently random calls. The destinations are not particularly high cost, but neither are they cheap. Countries like Vietnam, Laos, and other middle-priced Asian countries show up often. The traffic often appears to be to residential numbers.

TransNexus customers have reported tracing this type of fraudulent traffic coming from prepaid calling card companies operating a VoIP platform in an offshore colocation facility. Prepaid calling services are well suited to exploit this type of fraud since there are no calling numbers linked to customers. The IP address of the prepaid calling platform is the only link to trace the fraudster. Unfortunately, geolocation cannot always be used to identify the fraudster. These services can be offered via a tunnel through the Internet that hides the true IP address of the fraudster. The public IP address of the fraudster's calling platform could be the IP address of a hosted Virtual Private Network (VPN) service while the actual prepaid calling platform is located in a different part of the world.

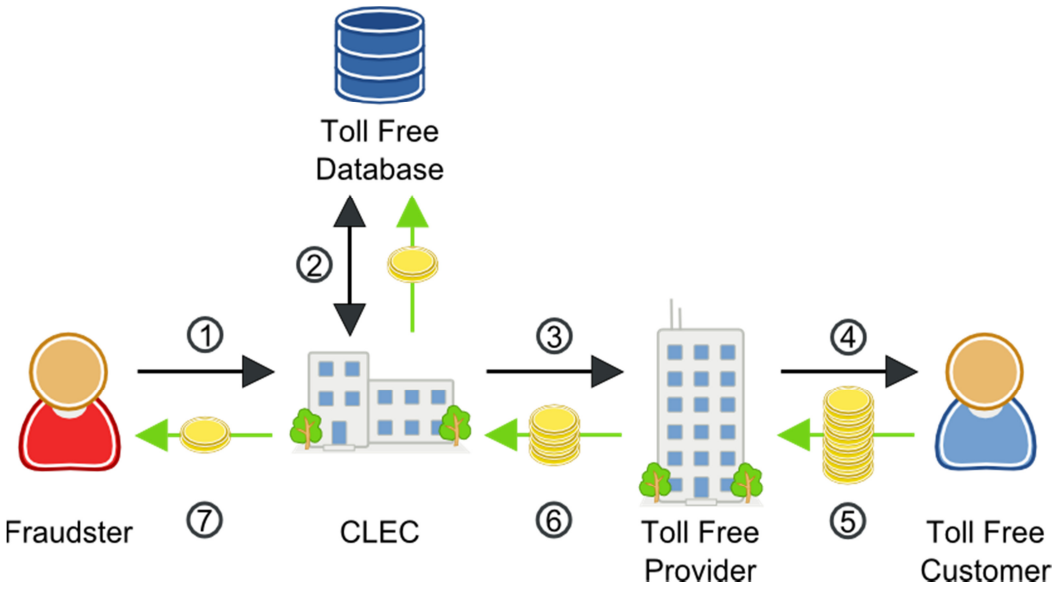
You can read more about this type of fraud in another TransNexus white paper, VoIP Theft of Service: Protecting Your Network.



Step	Call Flow	Money Flow
1	Fraudster steals credentials of the service provider's subscribers and registers with the service provider's softswitch using those stolen credentials.	
2	Fraudster's subscribers place a call.	Fraudster's subscribers pay for service.
3	(A) Fraudster sends INVITE to service provider's softswitch.	(B) Service provider's subscribers are billed for the call that was placed using their stolen credentials, but are unlikely to pay for the fraudulent calls.
4	Service provider routes calls to their destination.	Service provider must pay to complete the stolen call.

Toll Free Fraud

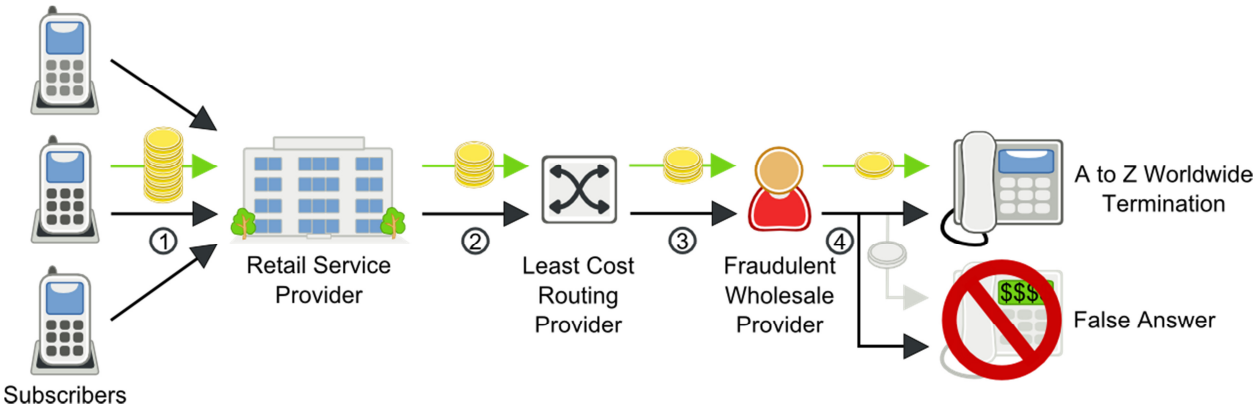
Toll Free fraud can affect any business that uses a toll free number. These calls are often left up for hours at a time and automated so multiple calls will be made at once. Fraudsters have gotten very sophisticated with this style of fraud, using different calling numbers for each call and only calling during business hours. They can navigate the IVR system to maintain a call for long periods of time, and vary the call duration so that the calls appear to be real traffic. When large companies, like financial institutions, are targeted, they frequently don't even notice the huge charges racked up by toll free fraud, even though they are expensive, long calls.



Step	Call Flow	Money Flow
1	Fraudster makes calls to toll free customer.	
2	CLEC makes a dip to the toll free database.	The CLEC pays to access the toll free database.
3	CLEC routes the call to the designated Toll Free Provider.	
4	Toll Free Provider completes the call to the Toll Free customer.	
5		Toll Free Customer pays the toll free provider the service fee.
6		Toll Free Provider pays the originating access fee to the CLEC.
7		The CLEC shares part of the access revenue with the fraudster who created the bogus toll free traffic.

False Answer Supervision

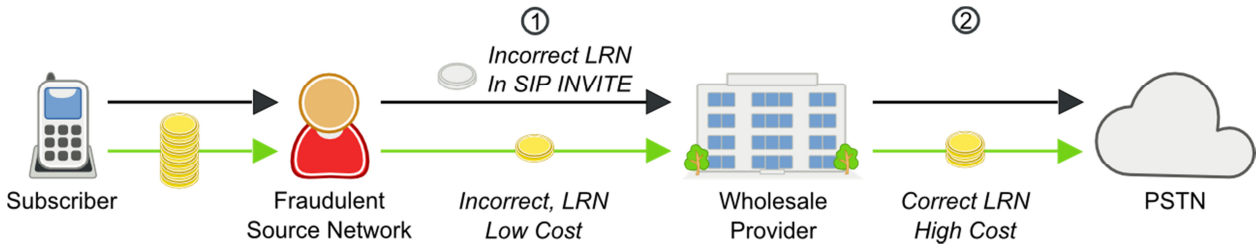
When a dialed phone number is not in service, the calling party will hear a brief recording telling them so. There is no answer supervision or connection between the calling and called party. Since the call never connects, it is an incomplete call and should not be billed. However, fraudsters use false answer supervision to make these calls appear as completed calls which may be billed. Perhaps the fraudster has published rates for terminating calls without any intention of actually completing the calls. Here, service providers will route calls through the fraudster, who, instead of terminating the call, will play a not in service message and then bill the service provider for more than 10 seconds of calling. This type of fraud hurts the originating service provider both by costing money, and by hurting their reputation.



Step	Call Flow	Money Flow
1	Subscriber makes a call.	The subscriber pays their retail service provider for service.
2	Service provider routes calls to its wholesale Least Cost Routing Provider.	The retail service provider pays their LCR provider.
3	The LCR provider routes the call to a wholesale provider.	The LCR provider pays the wholesale provider for a completed call to the high cost destination.
4	In most cases, the wholesale provider completes the call, but in some cases, the wholesale provider routes calls to the high cost destination with a “false answer” recording, not completing the call.	The wholesale provider pays nothing, because he did not actually complete the call to the high cost destination.

Location Routing Number Fraud

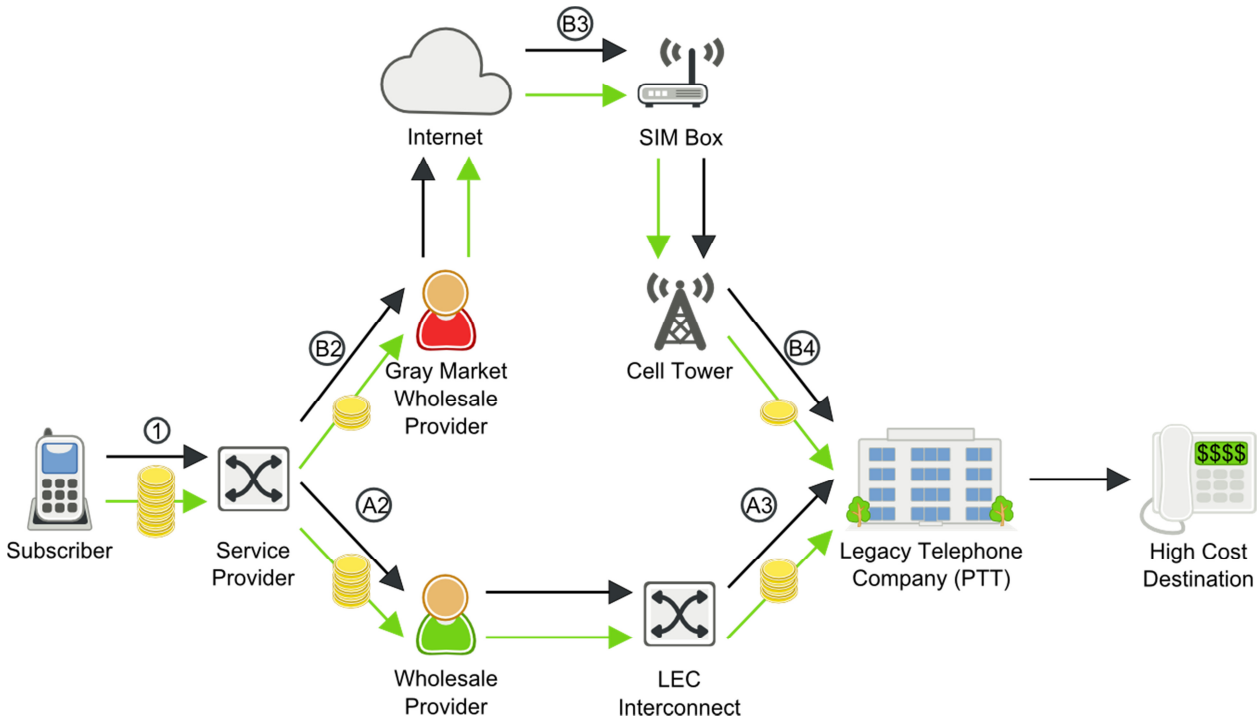
Location Routing Number Fraud or LRN fraud works based on the desire of some service providers to avoid extra charges from LRN "dips." Most providers will run an LRN dip to determine the correct LRN for a dialed number. However, some service providers will not perform an LRN dip if the LRN is already in the SIP message. Fraudsters take advantage of this by inserting the LRN for a relatively cheap terminating destination in their SIP INVITES, when the call is actually going to a high cost rural destination. The service provider will route and bill the fraudster using the LRN included in the SIP INVITE. The network that provides PSTN termination will route and bill for the call to the high cost rural destination using the correct LRN. The service provider will under-bill its customer for the call and will have to pay for the cost of the expensive rural call. In some cases, this can be up to 5x the price they billed the fraudster.



Step	Call Flow	Money Flow
1	Source Network sends a call to a wholesale provider with an incorrect low cost LRN in the SIP INVITE.	Provider charges the Source Network for a call to the incorrect LRN.
2	The provider completes the call.	The correct LRN for the call is more expensive than expected. The wholesale provider loses money, and the Source Network gets below cost termination.

Toll Bypass Fraud

Bypass fraud is the unauthorized insertion of traffic onto another carrier's network. In many countries, toll bypass for international call termination is criminal fraud. This scenario requires that the fraudsters obtain network access which makes international calls appear to be cheaper, domestic calls, effectively "bypassing" the normal payment system for international calling. One common technique for perpetrating this Interconnect fraud is GSM Gateway fraud, or SIM Boxing which is illustrated in the following diagram.



Step	Call Flow	Money Flow
1	Service provider has the choice to route a subscriber's call to a more expensive Wholesale Provider (A) or a lower cost "Gray Market" Provider (B).	Subscriber pays service provider for service.
A2	Service Provider routes call to Wholesale Provider.	
A3		Wholesale Provider pays a toll to the international Legacy Telephone Company (PTT).
B2	Service Provider routes call to a lower cost gray market wholesale provider.	The service provider pays the gray market wholesale provider.
B3	The gray market wholesale provider routes the call through a SIM Box.	
B4	The international call routed through the SIM Box to a cell tower looks like local subscriber traffic.	The gray market wholesale service provider pays a significantly reduced local traffic toll instead of the expensive international toll.

Inter/Intra State Tariff Bypass Fraud

Bypass fraud is the unauthorized insertion of traffic onto another carrier's network. Inter/Intra State toll bypass fraud attempts to bypass the higher tolls of intra-state traffic by making it look like inter-state traffic.

Step	Call Flow	Money Flow
1	Subscriber places an intra-state call.	Subscriber pays the service provider for service.
2	Fraudulent Service Provider changes the calling number of the call so that it appears to be a less expensive inter-state call.	The fraudulent service provider pays the wholesale long distance provider for an inexpensive inter-state call.
3	Wholesale Long Distance Provider routes call to the LEC as an inter-state call.	The wholesale long distance provider pays the LEC for the inexpensive inter-state call.
4	LEC completes the more expensive intra-state call, but charges for a less expensive inter-state call.	The LEC must pay for the more expensive intra-state call and loses money.

Schemes Conducted Over the Telephone

Criminals of all sorts use telephony as a tool to defraud consumers and businesses. "Phone fraud" is a huge category, and can cover anything from Nigerian prince style scams to identity theft to extortion. TransNexus does not offer a solution to protect against these types of fraud, though there are other solutions on the market that can.

Account Takeover

With this type of telecom fraud, the fraudster generally attacks something like a financial institution. Fraudsters will call financial institutions and maliciously impersonate another customer in order to steal the contents of an account. Pindrop Security estimates that a financial institution taking 50,000 calls per day will lose over $10 million per year to phone fraud losses.

Telecom Denial of Service (TDOS)

Telecom Denial of Service (TDoS) attacks are similar to traditional data network denial of service (DDoS) attacks. In a DDoS attack, unauthorized users flood a system with too many access requests, preventing

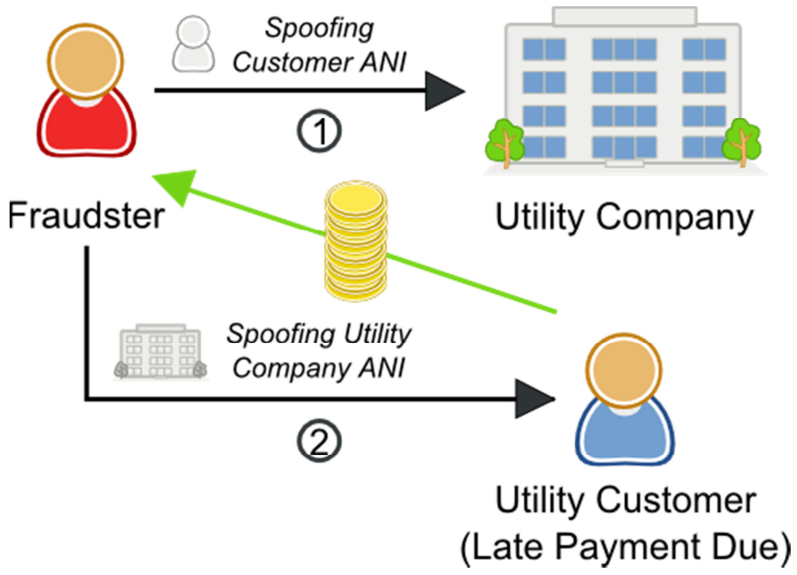
legitimate users from accessing the network. For TDoS, fraudsters make a huge number of phone calls, keeping them up for long durations, and overwhelming the capacity of an organization's phone network.

TDoS attacks can impair a voice network's availability, but can also be used as a tool for extortion. TDoS attacks have been in the news recently as a threat to public safety, as fraudsters have taken to using TDoS attacks against hospitals, police stations, and other public services.

Vishing

Phishing is a form of fraud that uses email messages with phony addresses, websites or pop-up windows to gather your personal information, which can then be used for identity theft. A form of phishing that uses the telephone instead of email is known as Vishing or "Voice-Phishing."

Vishers pose as a legitimate business to attempt to gather information from someone. That information can then be used for identity theft or other forms of fraud.



Step	Call Flow	Money Flow
1	Fraudster calls the Utility Company while spoofing the ANI of a customer. The fraudster then navigates the utility's phone system to gather customer data, especially credit balance.	
2	Fraudster calls customers who are behind on their payments while spoofing the utility company's ANI. The fraudster pretends to work for the utility company, and demands payment over the phone in order to get the customer's credit card information.	The fraudster now has access to the utility customer's credit card information and can use it to make fraudulent withdrawals.

TransNexus VoIP Fraud Detection Solutions

TransNexus solutions effectively eliminate the problems of traffic pumping fraud, PBX hacking, revenue sharing fraud, blind transfers, and call forwarding fraud for VoIP providers. The solution is to include smart monitoring that measures financial risk in near real time by Source IP, Calling Number, Customer ID, and by Detailed Dial Codes (country, state, mobile). TransNexus solutions send alerts or block calls when financial risk exceeds historical norms. TransNexus fraud detection features also include fraud blacklists, call diversion, and call blocking.

Summary

VoIP fraud is, and will remain, a lucrative criminal business. As VoIP continues to grow in popularity, schemes for beating the system will continue to become more complex and powerful. VoIP providers and enterprises must work together to ensure their networks are secure from every angle. By securing networks and analyzing traffic for signs of fraud, VoIP providers can minimize their fraud risks.

About TransNexus

TransNexus is a software development company specializing in applications for managing wholesale VoIP networks. TransNexus provides its Operations and Billing Support System (OSS/BSS) software platform to major VoIP carriers worldwide. Important carrier features offered by TransNexus are least cost routing, fraud detection, number portability, profitability analysis and QoS controls.

For more information, online demonstrations, and free downloads, please visit http://www.transnexus.com.