Wireless Attacks and Countermeasures

Wireless communication poses formidable challenges for the security professional.

Many wireless manufacturers design their devices for easy set up and use, often at the expense of sound security practices

. Many wireless devices default to little or no security

. A security professional must take extra precautions to protect sensitive data transmitted over wireless devices.

Two protocols that have been implemented to provide security for wireless communication are:

- *Wired Equivalent Privacy* (WEP) implements the 802.11 specification for wireless network connections.
- *Wireless Application Protocol* (WAP) is used with mobile devices such as PDA's and smart phones.

The following table describes weaknesses with both WEP and WAP:

Protocol	Vulnerabilities
Wired Equivalent Privacy (WEP)	WEP suffers from the following weaknesses: • The key is vulnerable during authentication. • The same WEP key is used for authentication and data encryption. • The WEP key is static. Because it doesn't change, it can be captured and broken. • Every host on the network uses the same key. • Key rotation is difficult. • WEP uses a very short *initialization vector (IV)* – • a mechanism that allows a cipher to • be executed in any of several streaming modes of operation • to produce a unique cipher text using the same encryption key. • The *integrity check value (ICV)* is easily defeated. • Unless you specify data encryption, all frames are sent in plaintext. • The RC4 encryption cipher could be replaced by a stronger encryption cipher. • The Service Set Identifier is broadcast. • Authentication can be open, meaning that identity is not checked. • Most wireless stations can be configured using the network name ANY.
Wireless Application Protocol /AP)	The most significant weakness of WAP is referred to *Gap in the WAP,* a security gap between a WAP client (handset) and a LAN host. The Gap in the WAP ack: • Exploits the decryption of transmissions at a carrier midpoint. • Compromises the carrier before the data is re-encrypted. • Exposes plaintext data. WAP deploys Wireless Transport Layer Security Protocol (WTLS) for authentication: • Class 1, Anonymous Authentication • Class 2, Server Authentication • Class 3, Two-Way Client and Server Authentication

Wireless networks are vulnerable to the following specific security attacks:

Vulnerability	Description
Eavesdropping	*Eavesdropping* is the most common threat of a wireless network. Wireless transmissions can be easily intercepted.
Site surveys or war driving	*Site surveys* or *war driving* are attempts by a hacker to scan the wireless networking area looking for unsecured access points or weak sswords.
Rogue access points or Man-in-the-ddle	*Rogue access points* or *man-in-the-middle* attacks occur when an attacker installs an unauthorized access point into your wireless network, allowing them to connect to the network.
Replay attack	In a *replay attack*, an attacker intercepts and records messages. The captured traffic is used at another time to try and recreate authentication. WEP, with its short initialization vector and static keys is susceptible to replay attacks.

Countermeasures for wireless communications are:

- First and foremost, treat a wireless network as though
- it were a publicly accessible network. Don't assume that the traffic on that network is private and secure.
- Put the access points in separate virtual LANs and
- implement some type of intrusion detection to help identify
- when an attacker is attempting to set up a rogue access point or is using a brute force attack to gain access.
- Encrypt all data transmitted through your access point.
- Set the access point to accept only Media Access Control (MAC) addresses.
- Use firewalls on each network access point.
- Avoid storing sensitive data on wireless machines whenever possible.
- Encrypt sensitive data that must be stored on the machine.
- Install security updates as soon as they are available.

Install antivirus software on the wireless computer.

Require that users connect to the wireless access point with a network cable when sending sensitive data.

- Disable the broadcasting of the SSID from all access points.
- Implement EAP-TLS to use different keys for encryption and broadcast traffic.
- Set the WEP broadcast traffic key to be renegotiated at a certain interval.

Set up a RADIUS server and a certificate authority. The RADIUS server authenticates the user back

against your network directory service.

Telecommunications fraud :

(aka **Telecom fraud**) represents a serious threat to the **telecommunication** industry.

It refers to the abuse of telecommunications products (mainly telephones and cell phones) or

services with the intention of illegally acquiring money from a communication service provider or its customers.

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. The

1. Traffic Pumping Schemes – These schemes use "access stimulation" techniques to boost traffic to a high cost destination, wh
2. Schemes to Defraud Telecom Service Providers – These schemes are the most complicated, and exploit telecom service provi and more.
3. Schemes Conducted Over the Telephone – Also known as "Phone Fraud," this category covers all types of general fraud that

Premium rate numbers

Many of the call scenarios featured in this report make use of premium rate numbers. These premium rate numbers are usu of the number will offer to share the revenue generated from calls to these numbers with anyone who sends them traffic. T 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 sha whom greatly increase traffic to a specific high cost destination. The destination then shares a portion of their profits with

The call signature for these types of scenarios are spikes in traffic to high cost destinations. Fraudsters often take advantag provider's customers. A customer whose network has been compromised will often refuse to pay large fraudulent charges, 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 PB 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 fron few customers ever pay for fraudulent calls and the service provider bears the financial loss because their carrier forces the

Multiple transfer fraud

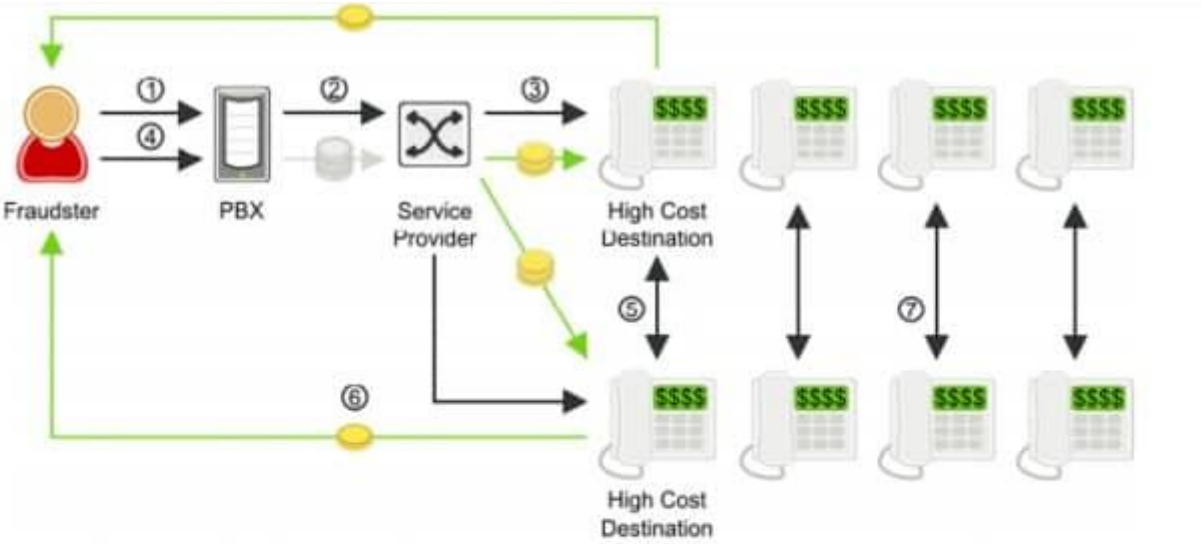
Multiple transfer fraud is an enhanced version of the previously described call forwarding fraud. In this fraud scenario, the immediately after the destination answers the call. When the call is transferred, the fraudulent call is in progress with two h hangs up. This fraud technique is especially harmful 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 thro

Most softswitches limit the maximum number of concurrent calls from a single customer. However, this call transfer fraud concurrent call limits since the call leg from the hacked phone source and the softswitch is very brief. A hacked customer

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 difficul transferred, they stay up until the carrier shuts it down. TransNexus customers report calls staying up for over 24 hours.



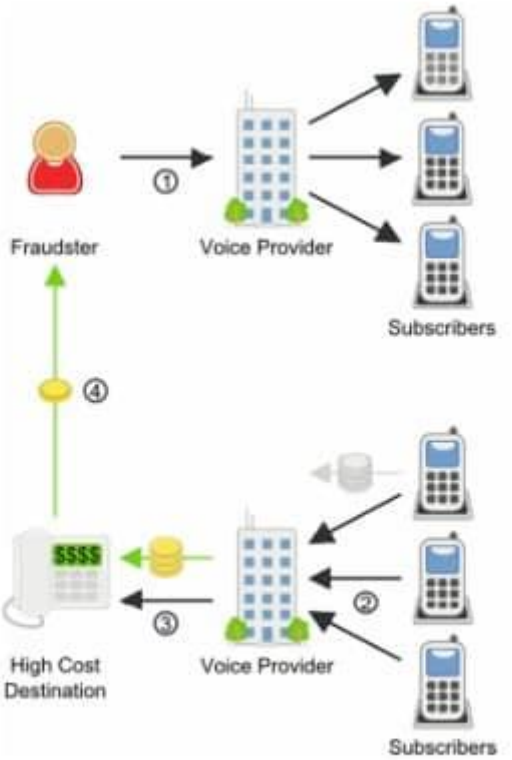
Step	Call Flow	Money Flow
1	Fraudster hacks an enterprise PBX to make calls to high cost destinations.	
2	Compromised PBX sends SIP INVITE to service provider's softswitch.	The hacked enterprise technically owes the service provider payment for these calls, but will rarely pay.
3	Service provider routes 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 to make money. A fraudster will set up a computer to dial a large number of phone numbers at random. Each rings just onc 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 dia used to generate calls to Caribbean countries that have the same dial pattern as calls to USA numbers. The number turns ou

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 fraudster isn't charged fo
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 technical provider payment for the but will not be happy to looked like a domestic nu
3	Service provider routes call to high cost destination.	The service provider mus fraudulent, high cost calls
4		The fraudster has a rever the high cost destination payment.

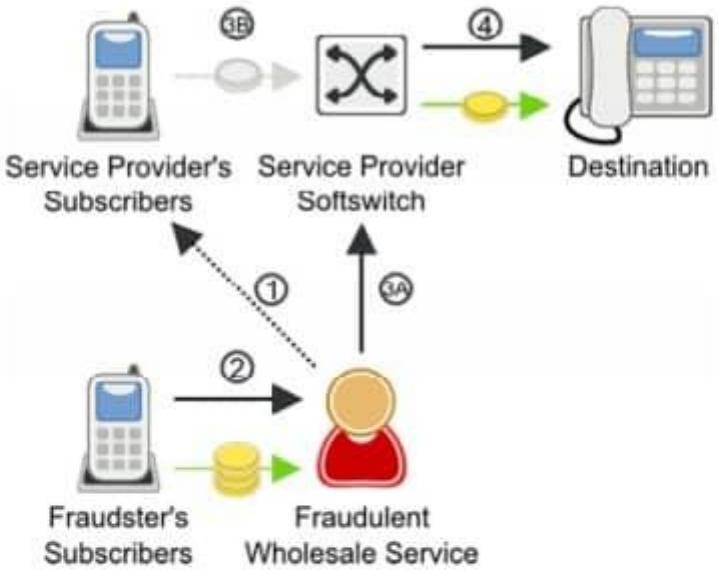
Schemes to defraud telecom service providers

Telecom Service Providers are particularly vulnerable to telecom fraud. Fraudsters are able to manipulate telecom regulato 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 making money by selling wholesale trunking services, using stolen credentials to terminate the calls. The key calling signa number of apparently random calls. The destinations are not particularly high cost, but neither are they cheap. Countries lik 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 op colocation facility. Prepaid calling services are well suited to exploit this type of fraud since there are no calling numbers l prepaid calling platform is the only link to trace the fraudster. Unfortunately, geolocation cannot always be used to identify offered via a tunnel through the Internet that hides the true IP address of the fraudster. The public IP address of the fraudst of a hosted Virtual Private Network (VPN) service while the actual prepaid calling platform is located in a different part of



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.

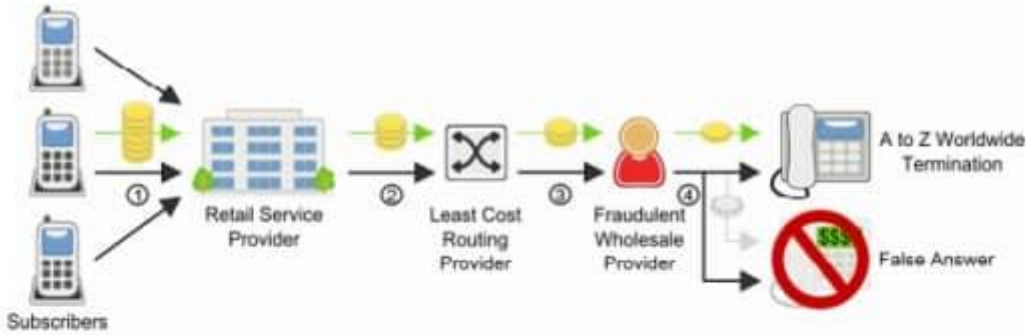
Toll free fraud

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 aut
once. Fraudsters have gotten very sophisticated with this style of fraud, using different calling numbers for each call and o
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
financial institutions, are targeted, they frequently don't even notice the huge charges racked up by toll free fraud, even tho

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 answ
calling and called party. Since the call never connects, it is an incomplete call and should not be billed. However, fraudster
these calls appear as completed calls which may be billed. Perhaps the fraudster has published rates for terminating calls w
the calls. Here, service providers will route calls through the fraudster, who, instead of terminating the call, will play a not
provider for more than 10 seconds of calling. This type of fraud hurts the originating service provider both by costing mon



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.

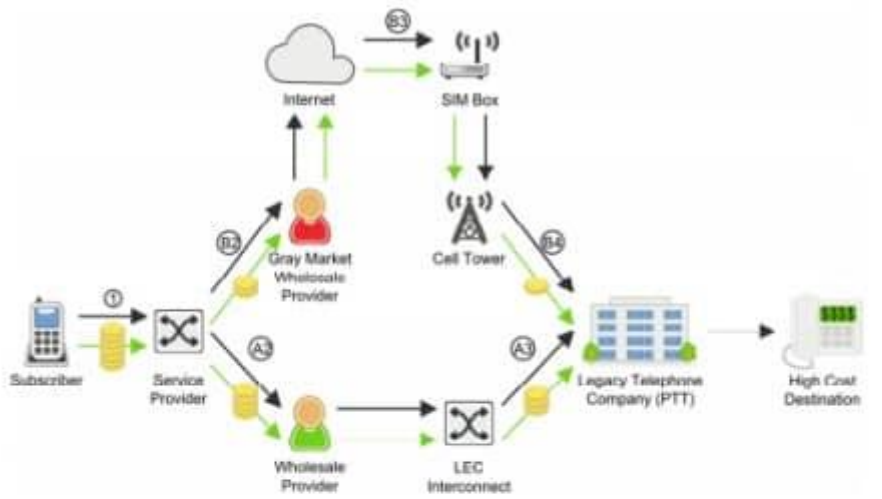
Location routing number fraud

Location Routing Number Fraud (LRN) fraud works based on the desire of some service providers to avoid extra charges f an LRN dip to determine the correct LRN for a dialed number. However, some service providers will not perform an LRN message. Fraudsters take advantage of this by inserting the LRN for a relatively cheap terminating destination in their SIP a high cost rural destination. The service provider will route and bill the fraudster using the LRN included in the SIP INVI termination will route and bill for the call to the high cost rural destination using the correct LRN. The service provider wi 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 fraudste

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 inter
This scenario requires that the fraudsters obtain network access which makes international calls appear to be cheaper, dom
normal payment system for international calling. One common technique for perpetrating this Interconnect fraud is GSM C
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/intrastate tariff bypass fraud

Bypass fraud is the unauthorized insertion of traffic onto another carrier's network. Inter/intrastate toll bypass fraud attemp
traffic by making it look like interstate 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 c style scams to identity theft to extortion. TransNexus does not offer a solution to protect against these types of fraud, thoug that can.

Account takeover

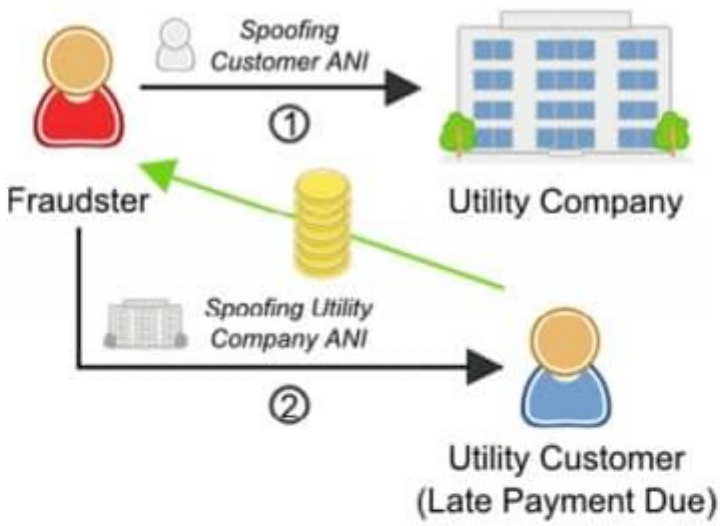
With this type of telecom fraud, the fraudster generally attacks something like a financial institution Fraudsters will call fir impersonate another customer in order to steal the contents of an account. Pindrop Security estimates that a financial institu over $10 million per year to phone fraud losses.

Telecom denial of service (TDoS)

Telecom Denial of Service (TDoS) attacks are similar to traditional data network denial of service (DDoS) attacks. In a DI system with too many access requests, preventing legitimate users from accessing the network. For TDoS, fraudsters make them up for long durations, and overwhelming the capacity of an organization’s phone network. TDoS attacks can impair a be used as a tool for extortion. TDoS attacks have been in the news recently as a threat to public safety, as fraudsters have hospitals, police stations, and other public services.

Vishing

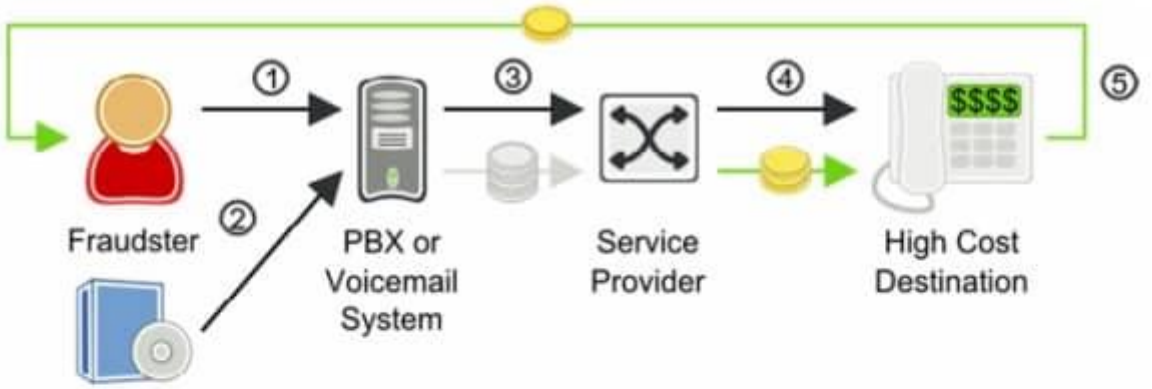
Phishing is a form of fraud that uses email messages with phony addresses, websites or pop-up windows to gather your per for identity theft. A form of phishing that uses the telephone instead of email is known as Vishing or “Voice-Phishing.” Vi attempt to gather information from someone. That information 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 telecom fraud prevention solutions

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



Call Generator

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.