Phone fraud

Phone fraud, or more generally **communications fraud,** is the use of telecommunications products or services with the intention of illegally acquiring money from, or failing to pay, a telecommunication company or its customers.

Many operators have increased measures to minimize fraud and reduce their losses. Communications operators tend to keep their actual loss figures and plans for corrective measures confidential.[1]

According to a 2011 survey by CFCA, an industry group created to reduce fraud against carriers, the five top fraud loss categories reported by operators were:[1]

- US$4.96 billion – compromised PBX/voicemail systems
- $4.32 billion – subscription/identity theft
- $3.84 billion – International Revenue Share Fraud
- $2.88 billion – by-pass fraud
- $2.40 billion – cash fraud

Contents

Types of frauds

Fraud against users by phone companies

- *Cramming* is the addition of charges to a subscriber's telephone bill for services which were neither ordered nor desired by the client, or for fees for calls or services that were not properly disclosed to the client. These charges are often assessed by dishonest third-party suppliers of data and communication service that phone companies are required, by law, to allow the third-party to place on the bill.
- *Slamming* is any fraudulent, unauthorized change to the default long-distance/local carrier or DSL Internet service selection for a subscriber's line, most often made by dishonest vendors desiring to steal business from competing service providers.
- *False Answer Supervision* is a misconfiguration of telephone company equipment, by negligence or design, which causes billing to start as soon as the distant telephone begins

ringing, even if a call is busy or there is no answer. The cost is typically subtle but recurring as subscribers repeatedly pay some small amount for calls which were never completed.[2]

Fraud against customers by third parties

- PBX dial-through can be used fraudulently by placing a call to a business then requesting to be transferred to "9-0" or some other outside toll number. (9 is normally an outside line and 0 then connects to the utility's operator.) The call appears to originate from the business (instead of the original fraudulent caller) and appears on the company's phone bill. Trickery (such as impersonation of installer and telecommunications company personnel "testing the system") or bribery and collusion with dishonest employees inside the firm may be used to gain access.
- A variant is a call forwarding scam, where a fraudster tricks a subscriber into call forwarding their number to either a long-distance number or a number at which the fraudster or an accomplice is accepting collect calls. The unsuspecting subscriber then gets a huge long-distance bill for all of these calls.[3]
- A similar scheme involves forwarding an individual PBX extension to a long-distance or overseas number; the PBX owner must pay tolls for all of these calls. Voice over IP servers are often flooded with brute-force attempts to register bogus off-premises extensions (which may then be forwarded or used to make calls) or to directly call SIP addresses which request outside numbers on a gateway; as they are computers, they are targets for Internet system crackers.
- Autodialers may be used for a number of dishonest purposes, including telemarketing fraud or even as War dialing. War dialers take their name from a scene in the 1983 movie WarGames in which a 'cracker' programs a home computer to dial every number in an exchange, searching for lines with auto-answer data modems. Sequential dialing is easy to detect, pseudo-random dialing is not.[4]
- In the US, owners of customer-owned coin-operated telephones (COCOTs) are paid sixty cents for every call their users make to a toll-free telephone number, with the charges billed to the called number. A fraudulent COCOT provider could potentially auto-dial 1-800 wrong numbers and get paid for these as "calls received from a payphone" with charges reversed.
- Autodialers are also used to make many short-duration calls, mainly to mobile devices, leaving a missed call number which is either premium rate or contains advertising messages, in the hope that the victim will call back.[5] This is known as Wangiri (literally, "One (ring) and cut") from Japan where it originated.
- 809 scams take their name from the former +1-809 area code which used to cover most of the Caribbean nations (it has since been split into multiple new area codes, adding to the confusion). The numbers look like Canadian or US telephone numbers but turn out to be costly, overpriced international calls that bypass consumer-protection laws which govern premium numbers based in the victim's home country. Some advertise phone sex or other typically premium content. Other variants on this scheme involve leaving unsolicited messages on pagers or making bogus claims of being a relative in a family emergency to trick users into calling the foreign numbers, then attempting to keep the victim on the line as long as possible in order to incur the cost of an expensive foreign call.[6]
- A more recent version of the 809 scam involves calling cellular telephones then hanging up, in hopes of the curious (or annoyed) victim calling them back.[7] Effectively, this is Wangiri but using former +1-809 countries such as 1-473 (Grenada) which look like North American domestic calls but are Caribbean island nations.[8]
- Pre-pay telephone cards or "calling cards" are also very vulnerable to fraudulent use; these cards contain a number or passcode which can be dialed in order to bill worldwide toll calls to the card. Anyone who obtains the passcode can dishonestly misuse it to make or to resell toll calls.

- Carrier access codes were widely misused by phone-sex scammers in the early days of competitive long distance; the phone-sex operations would misrepresent themselves as alternate long-distance carriers to evade consumer protection measures which prevent US phone subscribers from losing local or long-distance service due to calls to +1-900 or 976 premium numbers. This loophole is now closed.
- In the US, area code 500 and its overlays permit a "follow-me routing" in which, if the number has been forwarded to some expensive and arbitrary destination, the caller is billed for the call to that location. Similar issues existed with area code 700 as the numbers are long-distance carrier specific (except 1-700-555-4141, which identifies the carrier). Because of the unpredictable and potentially costly rate for such a call, these services never gained widespread use.
- Telemarketing fraud takes a number of forms; much like mail fraud, solicitations for the sale of goods or investments which are worthless or never delivered and requests for donations to unregistered charities are not uncommon. Callers often prey upon sick, disabled and elderly persons; scams in which a caller attempts to obtain banking or credit card information also frequently occur. One other variant involves calling a number of business offices, asking for model numbers of various pieces of office equipment in use (such as photocopiers) and sending unsolicited shipments of supplies for the machines, and then billing the victims at artificially inflated prices.
- Caller ID spoofing can be used to fraudulently impersonate a trusted vendor (such as a bank or credit union), a law enforcement agency or another subscriber. These calls may be used for vishing, where a scammer impersonates a trusted counterparty in order to fraudulently obtain financial or personal information.
- *Call clearing delays* in some United Kingdom exchanges may be abused to defraud. For obscure historical reasons, the system was designed so that a called party could hang up a call and immediately pick it up from another extension without it being disconnected. A fraudster would call a household and impersonate a bank or police; when the householder hung up and then attempted to call police or contact the impersonated party, the fraudster would still be on the line because the original call never properly ended.[9]
- Cordless phones are often even less secure than cell phones; with some models a scanner radio may intercept analogue conversations in progress or a handset of the same or a similar model as the target system may be usable to make toll calls through a cordless base station which lacks authentication capability. Obsolete analogue mobile telephones have stopped working in areas where the AMPS service has been shut down, but obsolete cordless phone systems may remain in service indefinitely.
- A recent scam involved Indian call centers targeting American or Canadian customers demanding "unpaid taxes" by impersonating government officials.[10] Similar government impersonation scams include the SSA impersonation scam.
- Every day, hundreds of scam calls are received on the US mainland which offer the recipients grant money from the Federal Government, but requesting a "small administration fee",[11] even though there are no fees associated with applying for or receiving a Government Grant.
- During the 1980s, a common form of premium-rate fraud involved manipulating children (often through television commercials, such as during Saturday morning cartoons) to call a premium-rate number without their parents' knowledge or permission, sometimes going so far as to ask a child to hold the phone receiver up to the television set as it played DTMF tones to automatically trigger the dialing of a premium number.[12] Such practices are now illegal in the United States.
- The Can You Hear Me? telephone scam was an alleged scam reported in the United States and Canada in 2017.

Fraud by phone companies against one another

- Interconnect fraud involves the falsification of records by telephone carriers in order to deliberately miscalculate the money owed by one telephone network to another. This affects calls originating on one network but carried by another at some point between source and destination.
- Refiling is a form of interconnect fraud in which one carrier tampers with CID (caller-ID) or ANI data to falsify the number from which a call originated before handing the call off to a competitor. Refiling and interconnect fraud briefly made headlines in the aftermath of the Worldcom financial troubles; the refiling scheme is based on a quirk in the system by which telecommunications companies bill each other – two calls to the same place may incur different costs because of differing displayed origin. A common calculation of payments between telecommunications companies calculates the percentage of the total distance over which each telecommunications company has carried one call to determine division of toll revenues for that call; refiling distorts data required to make these calculations.
- Grey routes are voice over IP gateways which deliver international calls to countries by mislabeling them as inbound local mobile telephone calls at destination. These "SIM box" operations are common in third world nations with exorbitant official international rates, usually due to some combination of tight control by one state-supported monopoly and/or excessive taxation of inbound overseas calls. Governments who believe themselves entitled to charge any arbitrary inflated price for inbound international calls, even far above the cost of domestic calls to the same destinations, will legislate against any privately owned, independent, competitive VoIP gateway, labeling the operations as "bypass fraud" and driving them underground or out of business. As a VoIP gateway in such a regulatory environment typically does not have access to T-carrier primary rate interface or PBX-style trunks, its operator is forced to rely on a hardware configuration with Internet telephony on one side and a large number of mobile SIM cards and handsets on the other to place the calls as if they were from individual local mobile subscribers.

Fraud against phone companies by users

- Subscription fraud: for example, signing up with a false name, or no intention to pay.
- Collect call fraud: most automated collect call systems allow the caller to record a short audio snippet, intended to identify the caller so that the recipient can decide whether or not to accept the charges. With the system being automated, the caller could insert any message they want, free of charge, as long as it fit within the short allotted time, and the recipient could refuse charges. A variant is to refuse a collect call at the higher operator-assisted rate, then call the person back at a lower price.
- Person-to-person call fraud: Under archaic operator assistance systems, a person-to-person call only charged a caller if they could reach a specific person at the other end of the line. Thus, if coordinated beforehand, a caller could use a false name as a code word, with the recipient rejecting the call, and no one would be charged.
- Intentional non-return of rental equipment (such as extension telephones) when relocating to a new address. The equipment would then be used at the new location without paying a monthly equipment rental fee. This has become rare as most telephones are now owned outright, not rented.

Frauds against phone companies by third parties

- Phreaking involves obtaining knowledge of how the telephone network operates, which can be (but is not always) used to place unauthorized calls. The history of phone phreaking shows that many 'phreaks' used their vast knowledge of the network to help telephone companies. There are, however, many phreaks who use their knowledge to exploit the network for personal gain, even today. In some cases, social engineering has been used to trick telecommunications

company employees into releasing technical information. Early examples of phreaking involved generation of various control tones, such as a 2600 hertz blue box tone to release a long-distance trunk for immediate re-use or the red box tones which simulate coins being inserted into a payphone. These exploits no longer work in many areas of the telephone network due to widespread use of digital switching systems and out-of-band signaling. There are, however, many areas of the world where these control tones are still used and this kind of fraud still continues to happen.

- A more high-tech version of the above is switch reprogramming, where unauthorized "back door" access to the phone company's network or billing system is used to allow free telephony. This is then sometimes resold by the 'crackers' to other customers.
- Caller name display (CNAM) is vulnerable to data mining, where a dishonest user obtains a line (fixed or mobile) with caller name display and then calls that number repeatedly from an autodialer which uses caller ID spoofing to send a different presentation number on each call. None of the calls are actually answered, but the telephone company has to look up every number (a CNAM database "dip") to display the corresponding subscriber name from its records. The list of displayed names and numbers (which may be landline or wireless) is then sold to telemarketers.[13]
- Payphones have also been misused to receive fraudulent collect calls; most carriers have turned off the feature of accepting incoming calls or have muted the payphones internal ringing mechanism for this very reason.
- Cloning has been used as a means of copying both the electronic serial number and the telephone number of another subscriber's phone to a second (cloned) phone. Airtime charges for outbound calls are then mis-billed to the victim's cellular phone account instead of the perpetrator's.

See also

- Caller ID spoofing
- Confidence tricks
- Credit card fraud
- Dial tapping
- Internet fraud
- Mobile phone spam
- Phreaking
- Traffic pumping
- Vishing
- Wire fraud
- Technical support scam

References

1. CFCA. "CFCA's 2011 Worldwide Telecom Fraud Survey" (https://m.usa-numbers.com/files/cfcas_2011_worldwide_telecom_fraud_survey.pdf) (PDF). CFCA. Retrieved 5 December 2011.
2. Bradford, Valerie (October 25, 2012). "Call Fraud Scenarios" (https://web.archive.org/web/20140220094021/http://freerouteserver.com/wordpress/2012/10/call-fraud-scenarios.html). *The TransNexus Blog*. Archived from the original (http://freerouteserver.com/wordpress/2012/10/call-fraud-scenarios.html) on 2014-02-20. Retrieved 2014-02-03.
3. "FACT CHECK: Call Forwarding Scam" (https://www.snopes.com/fact-check/call-forwarding-scam/). *Snopes.com*. Retrieved 9 May 2019.
4. "Sequential Calls" (https://www.cebodtelecom.com/features/sequential-calls/).

5. "You've got my number" (http://www.economist.com/node/1367988). *The Economist*. October 3, 2002. Archived (https://web.archive.org/web/20140203193811/http://www.economist.com/node/1367988) from the original on 2014-02-03. Retrieved 2014-02-03.
6. "Beware of Fraudulent International Phone Calls" (https://web.archive.org/web/20140207104315/http://www.bbb.org/us/article/beware-of-fraudulent-international-phone-calls-466). Better Business Bureau. 2004-04-07. Archived from the original (http://www.bbb.org/us/article/beware-of-fraudulent-international-phone-calls-466) on 2014-02-07. Retrieved 2014-01-29.
7. "BBB Warns of One Ring Cell Phone Scam" (https://web.archive.org/web/20140219220901/http://wisconsin.bbb.org/article/BBB-Warns-of-One-Ring-Cell-Phone-Scam-45593). Better Business Bureau in Wisconsin. 2014-01-29. Archived from the original (http://wisconsin.bbb.org/article/BBB-Warns-of-One-Ring-Cell-Phone-Scam-45593) on 2014-02-19.
8. Evans, Whitney (2014-01-01). "Scammers calling from 473 area code, police warn" (https://web.archive.org/web/20140220103952/http://www.ksl.com/?sid=28211799&nid=148&title=scammers-calling-from-473-area-code-police-warn). *KSL.com Utah*. Archived from the original (http://www.ksl.com/?sid=28211799&nid=148&title=scammers-calling-from-473-area-code-police-warn) on 2014-02-20. Retrieved 2014-02-03.
9. "Fraud prompts UK phone firms to tweak networks" (https://www.bbc.co.uk/news/technology-26559554). BBC News. 2014-03-13. Archived (https://web.archive.org/web/20140314014409/http://www.bbc.co.uk/news/technology-26559554) from the original on 2014-03-14. Retrieved 2014-03-14.
10. Zanane, Anant R. (2016-10-05). "How Workers From 9 Call Centres Near Mumbai Extorted Crores From Americans" (http://www.ndtv.com/mumbai-news/thane-call-centre-workers-pretended-to-be-irs-extorted-crores-from-americans-1470551?pfrom=home-lateststories). NDTV. Archived (https://web.archive.org/web/20161006052208/http://www.ndtv.com/mumbai-news/thane-call-centre-workers-pretended-to-be-irs-extorted-crores-from-americans-1470551?pfrom=home-lateststories) from the original on 2016-10-06. Retrieved 2016-10-05.
11. "Phone grant scam" (http://www.scamcallfighters.com/search-phone-grant-scam.html). *scamcallfighters.com*. Archived (https://web.archive.org/web/20170905141805/http://www.scamcallfighters.com/search-phone-grant-scam.html) from the original on 2017-09-05. Retrieved 2017-09-05.
12. Stern, Jane; Stern, Michael (1992). *Jane & Michael Stern's Encyclopedia of Pop Culture: An A to Z Guide to Who's Who and What's What, from Aerobics and Bubble Gum to Valley of the Dolls*.
13. "AT&T Says Data Miners Defrauded It" (https://www.courthousenews.com/2011/08/16/39024.htm). Court House News Service. 2011-08-16. Archived (https://web.archive.org/web/20140203075652/http://www.courthousenews.com/2011/08/16/39024.htm) from the original on 2014-02-03. Retrieved 2014-02-03.

External links

- OFCOM: Problems with your landline phone: slamming (https://web.archive.org/web/20070629203613/http://www.ofcom.org.uk/complain/landline/slamming/) - advice from the British communications regulator
- The Guardian: When slamming the phone prompts a row (http://money.guardian.co.uk/phones/story/0,13283,1466811,00.html)
- The Guardian: Orange slammed as users see red (http://money.guardian.co.uk/phones/story/0,,2109131,00.html) - concerns over data protection by British mobile telecom suppliers
- Bell Canada Fraud Control Centre (http://support.bell.ca/en-on/Home_phone/Long_distance_and_calling_cards/How_to_protect_against_long_distance_fraud)
- Anti-Deception Coordination Centre (https://www.police.gov.hk/ppp_en/04_crime_matters/adcc/contact.html) (Hong Kong)