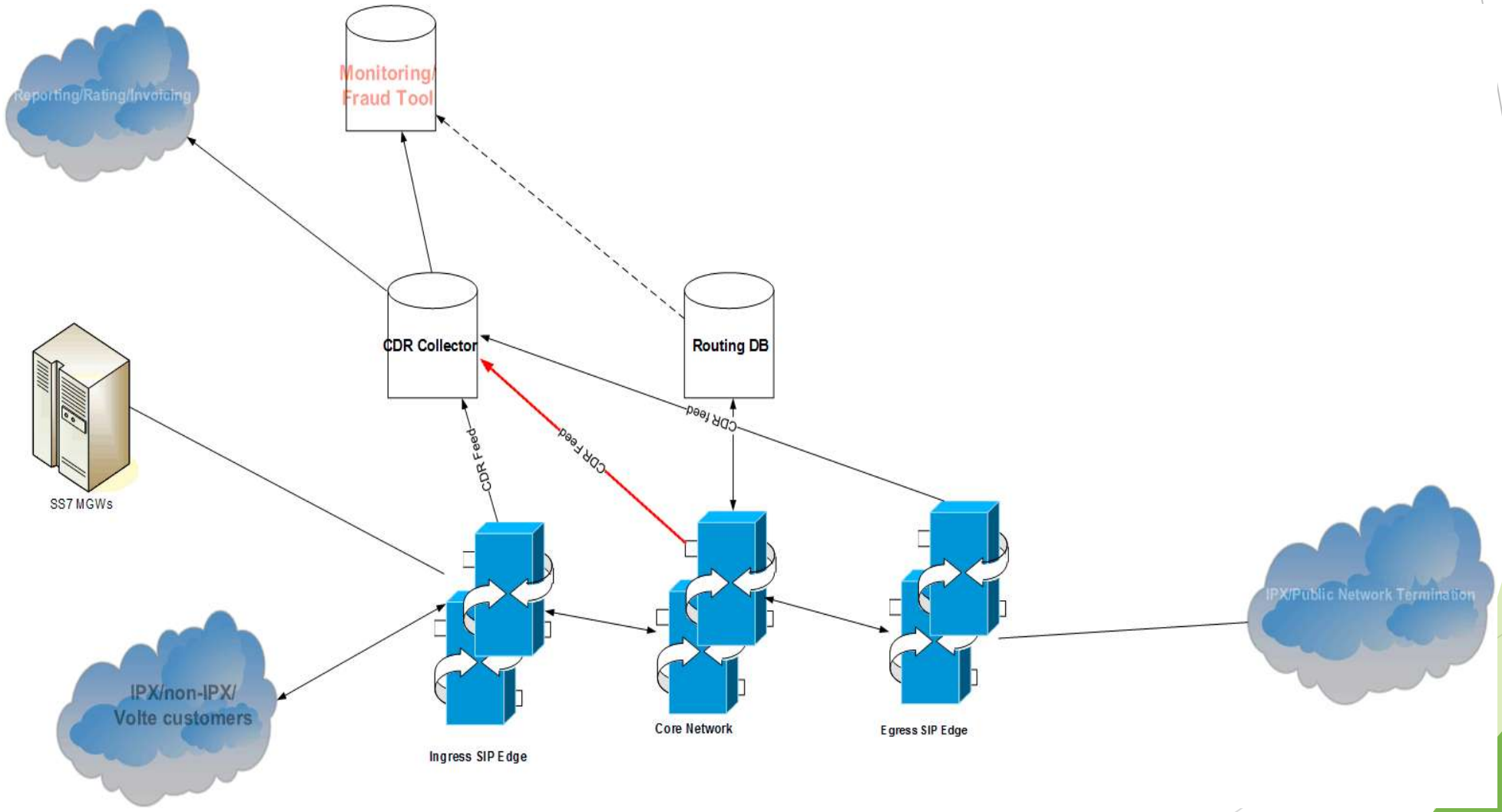
Voice Fraud in wholesale, A Carrier's perspective

Manpreet Singh

Director, Signaling Architecture, SW Development and Innovation

Typical carrier network



Potential fraud buckets?

- Legitimate user based fraud
- Fake or spoofed User based fraud
- Network based fraud
- Signaling Protocol based fraud

How does a legitimate user generate fraud?

- Subscriber buys an unlimited international calling plan (post paid)
- Make the account as a “shared” account for multiple people to use. OR
- Puts the SIM in a SIM box and start allowing IP based calls from various users.

How does carrier combat this?

- Create a real time map of specific A (calling number) to B numbers, including total minutes.
- Either generate or use pre-defined thresholds to create route exceptions.
  - Exception could include A number block or A number to called country block.
  - Generate a mid-call call kill operation to reduce the margin loss.

Fake or spoofed User based fraud

- A number is spoofed and doesn't belong to calling party. A number belongs to an unassigned number range or IPRN.
  - Number belongs to an expensive termination country (Wangiri like scam)
- Short A numbers or non e.164 format.
- Same A number to multiple B number dialing (IRSF)

How to combat?

- Manage the world wide assigned A number DB, locally or via external lookup.
  - Reject calls with certain error.
- Match the A number block to trunk its received on.
  - This will include number length and numbering format.
- In real time, find recurrence of certain A-B number recurrences and disconnect call in real time.
- Block terminations to premium destinations.

Network based-False Answer Supervision

- Either the transit network or far end network will signal call connection in ringing stage.
- Typically, the delta between ringing and connect is very small.
  - In SS7, ANM is received almost immediately after ACM/CPG
  - In SIP, 200OK to initial invite is received immediately after 180/183.
- User gets charged even when the phone was never answered.
  - In some case this is legitimate scenario where there are analog circuits.
- CDR analysis can be performed to detect and block
  - Analysis on ring to connect time delta. Large sample of short delta calls indicated FAS.
  - Input and output RTP packets can be analyzed for these calls. Larger packet count from called to calling Vs calling to called can indicate calls connected in ringing stage. (only to be done for short duration calls).

Signaling protocol related fraud?

- Use of different SIP headers in sending A number
  - From, PAID or RPID or a combination of all three.
- Especially causes issues when there are cases origin based charging.
  - Termination network may charge based on From or PAID or RPID but transit may charge differently.

How to avoid various charging models?

- Always normalize the number to PAID.
  - PAID takes highest preference for charging and make From same as PAID (except when privacy is requested).
  - Remove RPIDs if present and only send or insert (if missing) PAID
  - Expose the incoming From, PAID and RPID in the cdrs for post analysis.

Conclusion

- Fraud can manifest in different ways.
  - Via signaling
  - Via incorrect network behavior
  - Via end user and so on…
- Transit networks should try to standardize signaling based on real world use cases and specifications.
- CDRs analysis will surely help with reactive fraud blocks.
- Active call killing is crucial to avoid short burst of fraud calling.
- *if you want to stop fraud, think like a fraudster or make one your friend.*

Thank You..