David Morrow

Group Corporate Security Fraud Manager
Vodafone Group Services Limited

i3 forum
international ip interconnection

GSM Association Fraud Forum

Presentation to i3 Forum

David Morrow, Vodafone

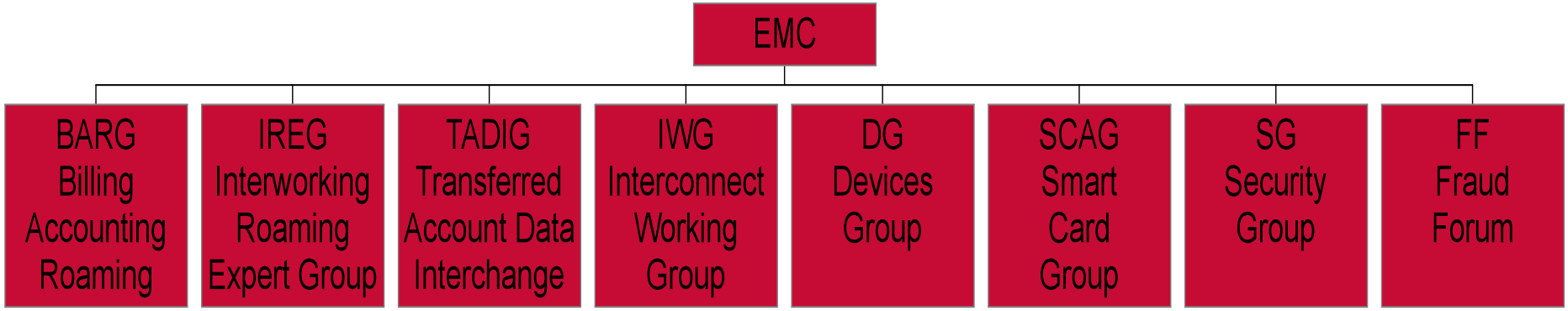
Document Number	
Meeting Date	17 May 2012
Meeting Venue	Chicago
For Approval	
For Information	X
Version	1
Security Restrictions	Confidential – GSMA Members, Associate Members & Rapporteurs & i3Forum members

GSM Association (GSMA) Background

- Global trade association responsible for GSM family of technologies
- Global membership of nearly 800 operators and 200 manufacturers and suppliers
- Organised into working groups and projects on many topics, open to all employees of GSMA member companies
- Participation leads to industry solutions, information sharing and education

GSMA Working Groups

- Eight Working Groups report to EMC
- Focus on a particular area of competence, e.g. security
- Deliver solutions for the GSM community where cooperation is needed, e.g. roaming
- Operators provide subject matter experts to the Working Groups
- HQ provides support via a WG Director and Coordinator



Fraud Forum (FF) – Objectives & Membership

- Trusted forum on GSM fraud issues to minimise exposure for members
  - Develop fraud awareness
  - Exchange intelligence & best practice
  - Develop & maintain industry countermeasures e.g. NRTRDE
  - Assess the fraud exposure of new services
  - Collaborate with other GSMA working groups and projects
- Provides value through **education** in addition to formal work items.

FF Membership – Jan 2012

	Total across FF, Asia-Pac FF & Africa FF
Individual members	487
Countries	106
Companies	242
Operators	199
Associate members	43

Evolution of Mobile Fraud

- Analogue - subscription fraud
- Analogue cloning - personal use, Call Selling (later inc. PBX fraud)
- Premium Rate Service (PRS) fraud (domestic)
- Roaming PRS fraud
- Credit card fraud – prepay
- SIM cloning (small numbers) + Roaming PRS, etc.
- International Revenue Share Fraud (IRSF)

Current key issues:

- Subscription fraud
- Roaming
- GSM Gateway/SIMbox (bypass)

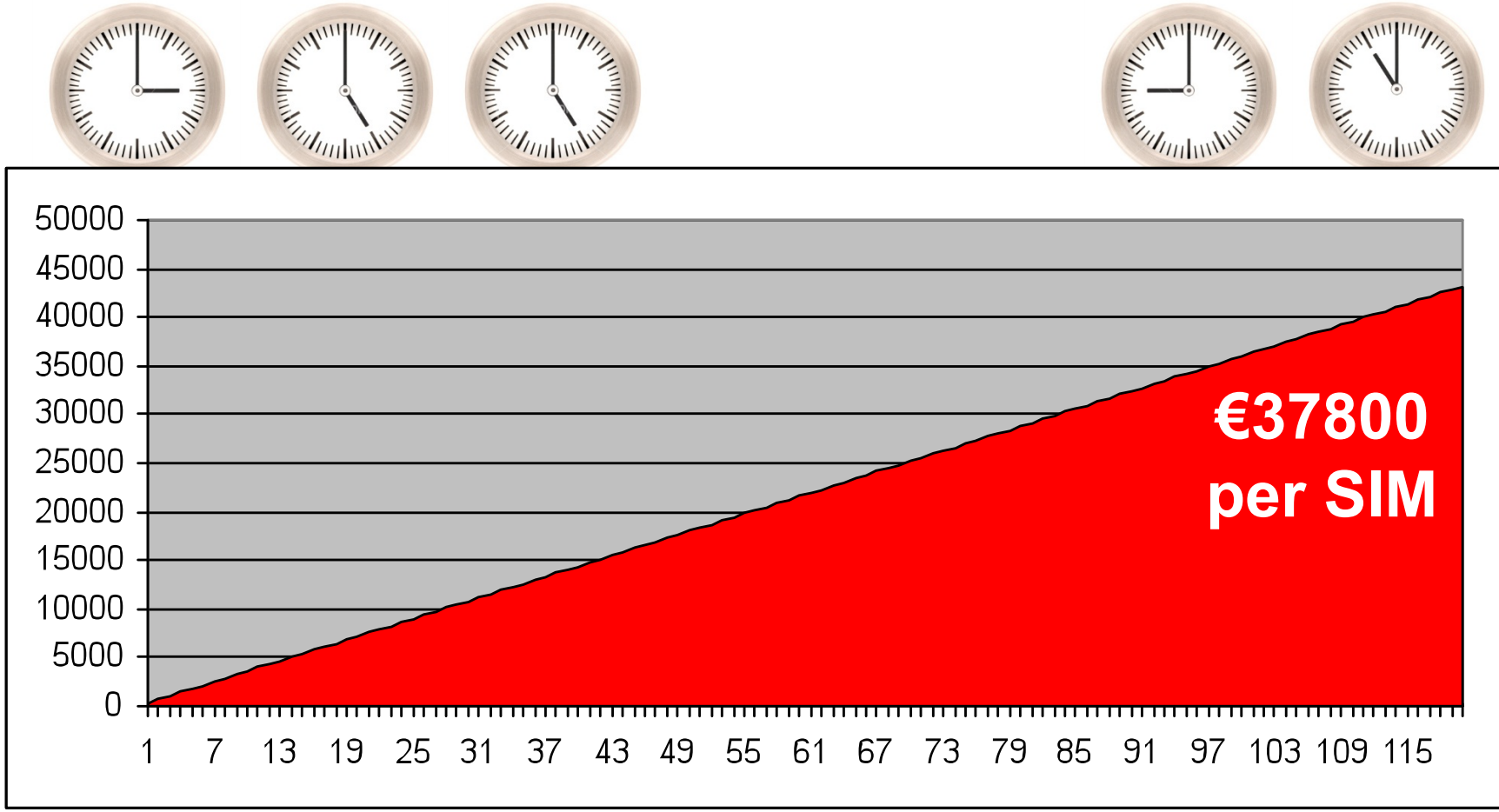
03:00 Thurs

05:00 Thurs

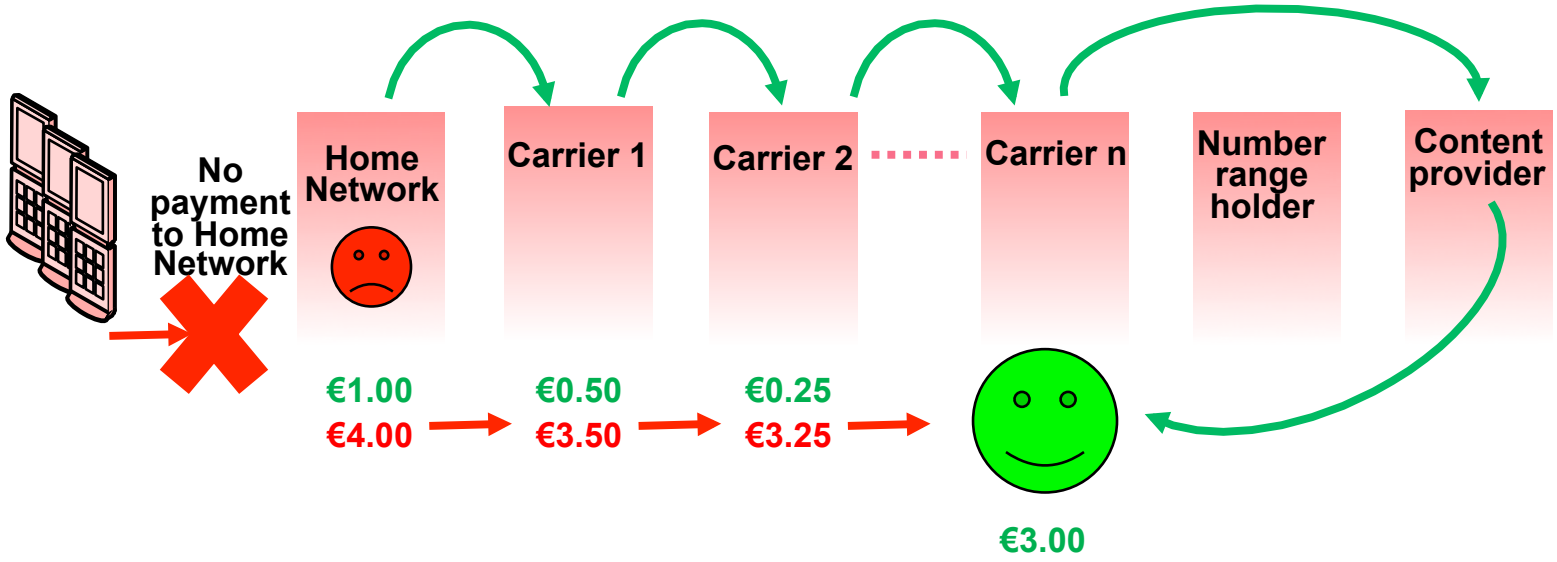
17:00 Fri

09:00 Mon

11:00 Mon



Optimised Fraud



- Short – stopping by fraudsters
- Number Range hi-jacking

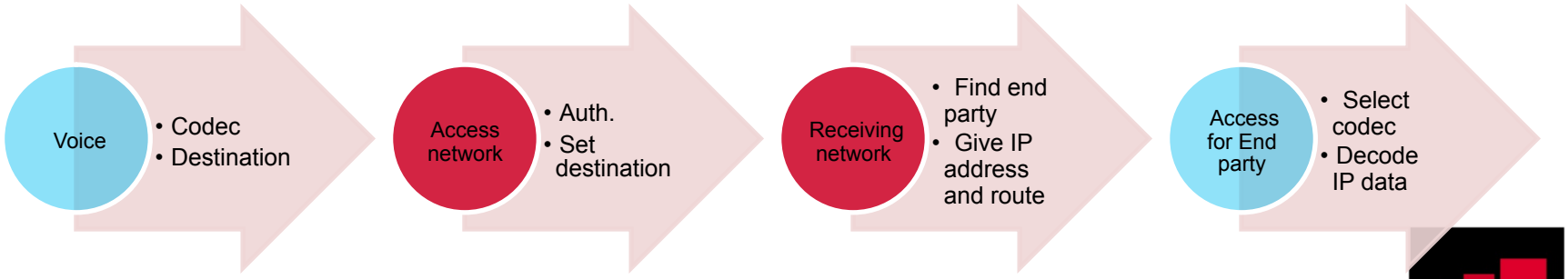
What next (and what's in a name)?

- 4G
- LTE (Long Term Evolution)
- NGN (Next Generation Networks)

- all terms referring to mobile evolution from circuit switched to packet switched services

What is a Next Generation Network?

- Support for services, applications based o
- Interworking with legacy networks via open interfaces
- Unified service
- Converged services
- Services don't have to be from the Mobile Operator



IP & IMS Systems

- First time in mobile telecoms that the bearer providing the service is totally separate from the services offered
- In effect, this means two separate operators can run services, one for the service and one for the bearer
- Within 10 years Telco networks will be solely IP backbone and conventional switching will have disappeared due to cost
- All services offered will be digital

12

NGN issues - Identity Management

- There are now two types of identity - for the bearer & service layers
- Different identities may be combined into one account
- There will be a number of other identities used internally in the network
- Many of the identities are dynamic and change in session

Service Identity

IMPU
IMPI
sip_uri
tel_uri
E.164

Bearer Identity

- Account ID, Radius ID
- IMSI, Terminal ID
- MSISDN, Fixed line access number
- IMEI, Device Electronic serial number

NGN: The Challenges

- The key areas for challenges and risks are:
  - For Operators - control of separate Bearer and Services
  - Service Providers - lack of total control and information
  - New players with lack of knowledge and/or experience
  - Fraud Management - new technical opportunities for fraud
  - Revenue Assurance - Different billing models and data sources
  - Security - More complex technical controls
  - 3rd parties - Control and trustworthiness of billing and content!

- A mix of:
  - More complex technology
  - Different billing models

So Fraud will be different

IMS: IP Multimedia Subsystem

- IMS means a complete new network that separates the bearer network and can work across many network types
  - Mobile GSM, 3G, CDMA etc.
  - Fixed networks
  - WLAN
  - PAN e.g. Bluetooth, IR or Near Field Communications (NFC)

- IMS does not standardise applications, but aids access of multimedia & voice applications across wireless & fixed terminals
- IMS provides 'horizontal control layers' that allows the separation of the access/bearer network from the service layer

- **This drives different needs for fraud & risk management**

15

Customer Terminal Device

- In NGN, the “end point” can be called different names in different network types can be:
  - Mobile Phone (GSM, CDMA, …..)
  - Data terminal – tablets or smartphones
  - ASDL or Cable Router/ Modem
  - IAD (Integrated Access Device)
  - CPE (Customer Premise Equipment) for fixed networks

- They all have some common functions:
  - Store an identity such as SIP Username and password
  - Have an IP address (allocated or dynamic)
  - Have some other identity such as an equipment identity
  - Have an operating system and memory and run applications
  - Generally poor internal security or fraud controls so these need to be in the CSP’s systems

Key Issues for Next Generation Services

- Every service can be very different and made up of different component parts - both IP with interaction over different **Bearer** and **Services**
- Content and payments will move operators to a different risk profile similar to those of banks and retailers – e.g. money laundering, undelivered goods etc.
- Issues for the operator on CPE, IAD, SIP & smartphones and the applications that exist on them – corruption or malware
- Proof of the location and identity of the user and transaction is difficult with mobile and IP based services!

NGN Service Groupings

Professional:
- Video Conference
- Multimedia Sales
- Advertising
- Informative
- Remote Vigilance
- Mobile Marketing
- On Line Training
- Location Based
- Security Surveillance
- Mobile Office
- Presence

Financial:
- M – Commerce
- Virtual Banking
- E – Payments
- On Line Billing
- Stock broking
- Auctions
- Government
- Community
- Financial Transactions

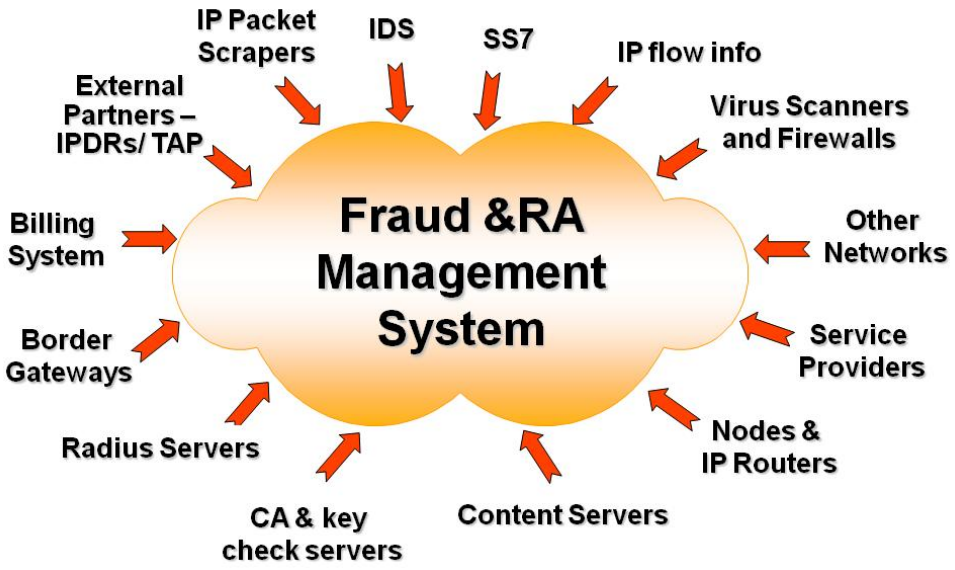
Entertainment:
- Informative
- Multiparty Gaming
- Music
- Movies
- Video Content
- Gambling
- TV
- Radio
- Pictures
- Messaging
- Video Sharing

Shopping:
- M – Commerce
- Auctions
- Retailing
- Ticketing
- Booking
- Working
- Advertising

18

Challenges for Fraud & RA

- More complex both from a technical and operational perspective
- Data more real-time and complex - increased need for the collection of events
- Linking data in Bearer & Services
- Requires new data feeds from new services platforms



NGN Frauds?

- Aim for the highest value content or greatest volume
- Hackers and Malware writers looking for notoriety by implementing widespread damage / maximum financial gain
- Fraudsters from the Finance Industry targeting M-banking & M-commerce
- Will make more use of internal information and work with internal staff due to better external controls
- Criminals will exploit the same approaches as today but with a greater potential reward….. Moving away from simple airtime usage – comparatively low value!

NGN Fraud Management Approach

- NGN FM approach will be a variation of what is done today, but it will be more complex both from a technical and operational perspective
- Significantly more data and increased need for the collection of events from many places compared to present
- The identities may not have a known location for traffic origination or termination? 20% of IP are not where they are geographically expected
- Traffic can originate in different places - no need for a central switch location where call records can be collected for FM purposes

Services Fraud Management

- Fraud detection of the services layer will be partly the same as today - many services used combined with multiple bearers
- Provisioning related fraud will need detecting as a lot more self care will take place and it will also be driven by the billing model
- FMS will need to know which services the customer is allowed to use - needs much more control of provisioning fraud than with present systems

Fraud Control & Management Panel Discussion

Panelists:

Dima Alkin, Director, Sales Support, North America, Cvidya

Peter Coulter, Member of Executive Cmtee-FIINA, Executive Director, Global Fraud Management, AT&T

Steve Heap, Senior Technology/Communications Executive, IPSoft

David Morrow, Group Corporate Security Fraud Manager, Vodafone Group Services Limited

Thomas Walker, Director - Business & Solutions Consulting, Subex

i3 forum
international ip interconnection

3rd Annual i3Forum Conference

The Future is All IP

May 17, 2012
Chicago

www.i3forum.org

i3 forum
international ip interconnection