

**ORACLE®**



## **Enterprise Security – Cyber Security APAC Forum**

David Louey Gung

Director Justice & Public Safety APAC



# Agenda

- Police Security Requirements
- Major Challenges for Law Enforcement Agencies
- Oracle Enterprise Security Solutions
- Innovative secure solutions for Disaster Management– Case Studies

# Victoria Police IT infrastructure - Security Requirements

- In 1993 the current HRMS and Operational Police RMS were implemented on the Mainframe.
- Very little technology existed in the 380+ police stations
- Uniformed police developed their own local applications and (standalone) LANs at 20 stations.
- 1999 IT infrastructure rolled out
  - Shared Govt WAN – VPN
  - Standard LANs, servers & desktops installed
  - Username/Password access validated from HRMS
  - Password resets highest no. H/desk Calls (single sign-on)
- 2001 (ROI) - Oracle Financials & Website implemented
  - Security Report showed ~80K attempted breaches/month
  - Penetration test commissioned → security weakness



## Victoria Police Applications - Security Requirements

- 2004 Centralized Managem't of Apps.(20 to >400)
  - Few complied with Security Policy & Privacy Law
  
- Inappropriate use of police information
  - Police Officers who breached security and privacy policies disciplined / heavy fines
  
  - Reason for LEAP/RMS access implemented
  
  - All LEAP/RMS changes audited (separate to DB audit records)
  
  - LEAP/RMS Audit records analyzed regularly by police auditors to determine cases of appropriate use.

## Security Requirements Victoria Police



- **2004 Crime Dept evaluated Enterprise Investigative Case Management solutions for intelligence gathering to address major crime:**
  - **Security considerations the No. 1 requirement.**
  - **Restrict Case Access to Investigating Team**
  - **Team Lead to nominate team members' access**
  - **Senior team members only to access certain info**
  - **Hide info. from Systems Administrator & DBA**
- **Enabled Internal Investigations to migrate across**

# Major Challenges for Law Enforcement Agencies

- Major Challenges are:
  - Organised Crime
  - Terrorist Activity
  - Cyber Crime
- Transnational nature, create global issues that become domestic issues
- Oracle has dedicated resources with domain expertise and technology solutions to assist Law Enforcement agencies address these challenges.





# The Challenges We're Hearing

## Fragmented Police and Intelligence Information

**“How can we create a trusted environment for the sharing of critical information across departments and jurisdictions?”**

Clues and evidence related to criminal or terrorist activity are often spread across disconnected databases and paper files stored in thousands of law enforcement databases.

Gartner, Facing Information-Sharing Challenges Among Law Enforcement Agencies

## Inability to Analyze and Act on Crime Information

**“How can we identify trends and patterns to anticipate and prevent incidents?”**

Organizations should designate a group of individuals to be responsible for collecting and analyzing crime information and other performance-related data to improve an agency's understanding of the incidence of crime and how an agency combats it..

Gartner, Take These Four Steps When Adapting Your Organization to the CompStat Model

## Limited Resources

**“How can we reduce crime and combat terrorism with limited resources?”**

Police forces are now dealing with crime that would be unrecognizable to police officers of a generation ago and must do so with a rapidly shrinking resource base.

# Oracle – > 30 Years of Security Leadership

1977

2009

Audit Vault  
Database Vault  
Content DB, Records DB  
Secure Enterprise Search  
Thor & Octet String (IdM Acquisitions)  
Phaos, Oblix, (IdM Acquisitions)  
Database CC Security Eval #18 (10g R1)  
Transparent Data Encryption  
VPD Column Sec Policies  
Fine Grained Auditing (9i)  
1<sup>st</sup> Database Common Criteria (EAL4)  
Oracle Label Security (2000 8.1.7)  
Virtual Private Database (1998)  
Enterprise User Security (8i)  
Database Encryption API  
Kerberos Support (8i)  
Support for PKI  
Radius Authentication  
Network Encryption (Oracle7)  
Oracle Advanced Security introduced  
First Orange Book B1 evaluation (1993)  
Trusted Oracle7 MLS DB  
Government customer (CIA – Project Oracle)

ORACLE

# Oracle in Justice and Public Safety

Did You Know?



**8 of the top 10** largest Law Enforcement Agencies in the U.S. And Canada use Oracle Technology and/or Applications



**15 of the 25** European Union Member Nations run Oracle Applications



**9** Asia Pacific Country Governments run Oracle Applications



The U.S. and Canadian Intelligence Communities and Departments of Justice run Oracle

ORACLE

# Oracle's Justice and Public Safety

21st Century Next-Generation Justice & Public Safety Information Systems

## Integrated Justice Community Collaboration

Citizen Portals

Community Outreach

National, Regional & Local Law Enforcement

Cross Jurisdictional Law Enforcement

Cross Jurisdictional Intelligence

## Overlay Infrastructure for Investigation, Apprehension, Prosecution and Emergency Response

Analytics & Business Intelligence

Business Process Management

Master Data Management

Unified User Interface

Data Integration Services

## Law Enforcement

Intelligence Gathering and Analysis

Investigative Case Management

Evidence Management

Emergency Preparations & Response

## Courts

Litigation Case Management

Jury & Trial Management

E-Filing & E-Discovery

Court Records Management

## Corrections

Offender Management

Prison Records Management

Community Programs

Prison Management

## Border Control

Surveillance

People & Cargo Entry & Exit Management

Customs & Excise

Immigration and Asylum Management

## Administration & Enterprise Management

IT Services (Help Desk, Etc.)

Human Resources & Workforce Management

iLearning & Classroom Training

Facilities Management & Field Service Auto.

Performance Management & GRC

Financial Management

Grants Management

SCM & Procurement

Records Management

Program / Project Management

## Infrastructure

Identity Management & Security Services

Data & Content Management

Mobility & Location Services

Service Oriented & Event Driven Architecture

Highly Available and Scalable App & Info Svcs



# Investigative Case Management

## Reduces Administrative Time for Front Line

### Lead Management

- Use as a secure collaboration tool, natively tied to a case
- Route to the right resource for follow-up and view as part of the parent case

### Evidence Management

- Track all forms of Evidence & provide secure visibility to all parts of the organization
- Tie to “hard” assets

### Incident Management

- Capture complete law enforcement information on external events
- Convert to case and spawn requests for service

### Offenses

- Enter and track all crimes that the perpetrators allegedly committed as part of the incident (“assault”)

### Locations

- Track specific locations using GPS coordinates or community nicknames (“the old mill”)

### Subjects

- Track individuals whose names are unknown, but statistics are known (“john doe”)

### Offenders

- Track known perpetrators of criminal offenses

### Circumstances

- Track the “soft” issues or aggravating factors that surround a case (“alcoholism”)

### Suspects

- Contextual to a case, track all suspects

### Identities

- Track multiple aliases of individuals in the system

### Arrests

- Track arrests made in course of an incident investigation
- Arrests are tied to individuals

### Victims

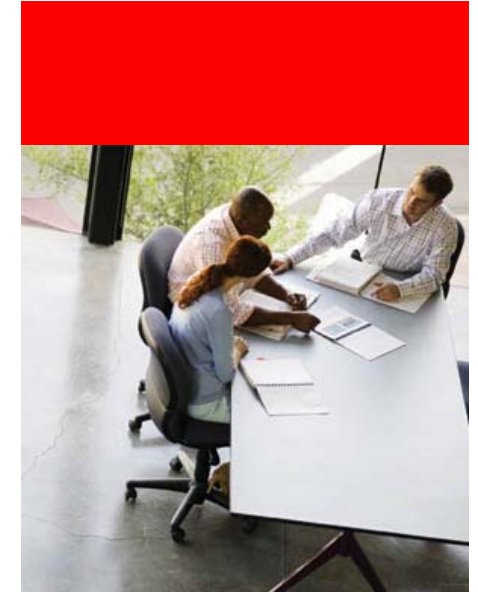
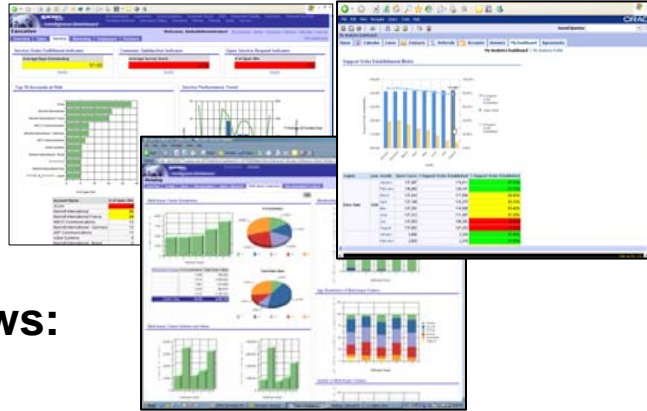
- Track victims in the context of offenses or incidents

# Business Intelligence

Identifies Crime Trends, Patterns and Clusters

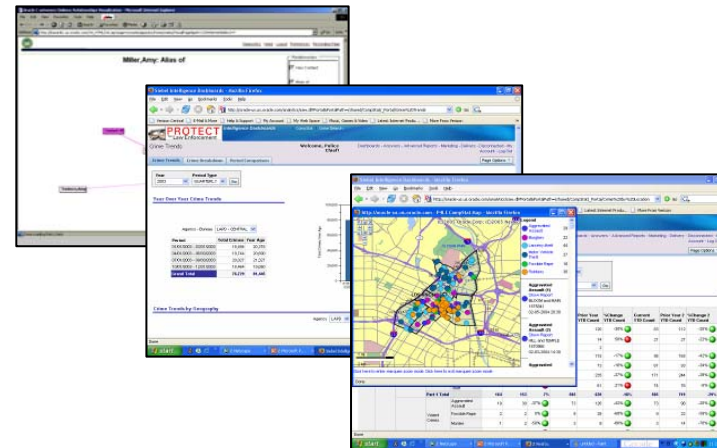
## Performance metrics

- Pre-defined Executive dashboards
- 'Real Time', Regional Data
- Aggregate & Summary Views:
  - Comparative
  - Drill Down
  - User defined thresholds



## Transactional

- Executive, Crime Analysis, and Counter Terrorism Dashboards
- 'Real Time', Regional Data
- Aggregate & Summary Views:
  - Crime Reports, Emergency Calls,
  - Contact Cards, Citations, Warrants,
  - Probation, Parolees, etc.



ORACLE

# Daon/Oracle – The Open Identity Platform

- Examining the constituents of an “Open Identity Platform”



# Oracle Adaptive Access Manager

- Web access real time fraud detection
- Provides online authentication security consumers and enterprise employees.
- Strong security that ensures business is compliant with regulatory requirements:
  - Payment Card Industry Data Security Council (PCI DSC) and
  - Federal Financial Institutions Examination Council (FFIEC) for online interaction.
- Protects against attacks such as phishing, Trojans, viruses, fraudulent transactions etc.
- Used in 70 countries, 30 M people





# Immigration & Customs Enforcement (ICE) Cyber Crime Centres (C3)

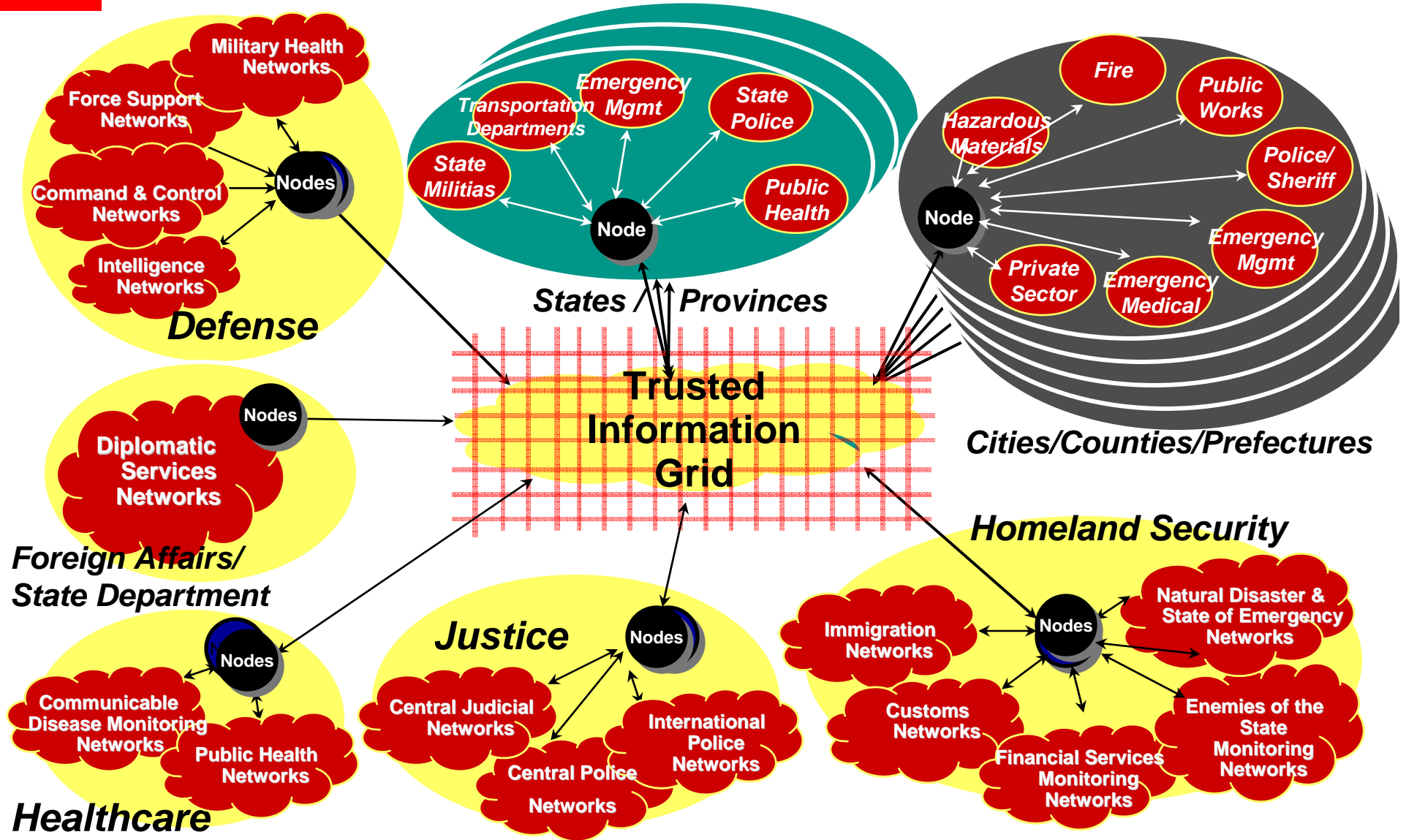
- Using Oracle's COTS CRM products, database and related portal development tools, ICE combats crimes committed online and electronically, providing a new avenue through which to pursue criminals, predators and child pornographers
- Enabled collaboration with external Law Enforcement officials throughout US - contributed to arrest of 5, 400 child sex predators plus deportation of 2,000 - <sup>st</sup> yr
- enables online access to information to help its agents combat child pornography, money laundering and trafficking of arms, drugs and stolen art as well as intellectual property rights violations.
- C3 investigates domestic and international criminal activities occurring on or facilitated by the Internet.
- Federal agents working on those cases avoid delays, log into the C3 portal, create a case, enter information about suspected targets in a case file.
- Create a summons on-line
- nightly importation of tips (along with images & evidence) from the National Center for Missing and Exploited Children (NCMEC) enables C3 to proactively investigative leads
- C3 requires systems featuring industry standards, sharing of info via open standards XML & high levels of security so victim information is protected and access based on authorization and need to know
- Greater efficiencies - hours saved can be significant in terms of a child's safety



# Intelligence Fusion Centers

- US Fed Govt post event analysis concluded that sufficient information existed such that Law Enforcement officials could have intercepted the terrorists that flew aircrafts into WTC.
  - Philosophy relies heavily on real-time information integrated into single comprehensive 360 view
- Funding & establishment of intelligence is a direct result of need for better, more integrated info. about suspects, locations etc that may be used in planning a crime , including a terrorist act
- Effective & Efficient mechanism to exchange information & intelligence
- Post 911 public sector mandated to transform from “need to know” to a “need to share” community (incl nationally sensitive info.)
- Improve ability to fight crime & terrorism by analyzing data from a variety of sources & dbs (tips, leads, driver license, vehicle reg. etc)
- Enables detection, deterrence and prevention of future terrorist attacks
- Operational configurations: regional –sharing info. among states; vertical structure –connecting states to federal agencies but not to other states.

# The Concept of a Network of Networks



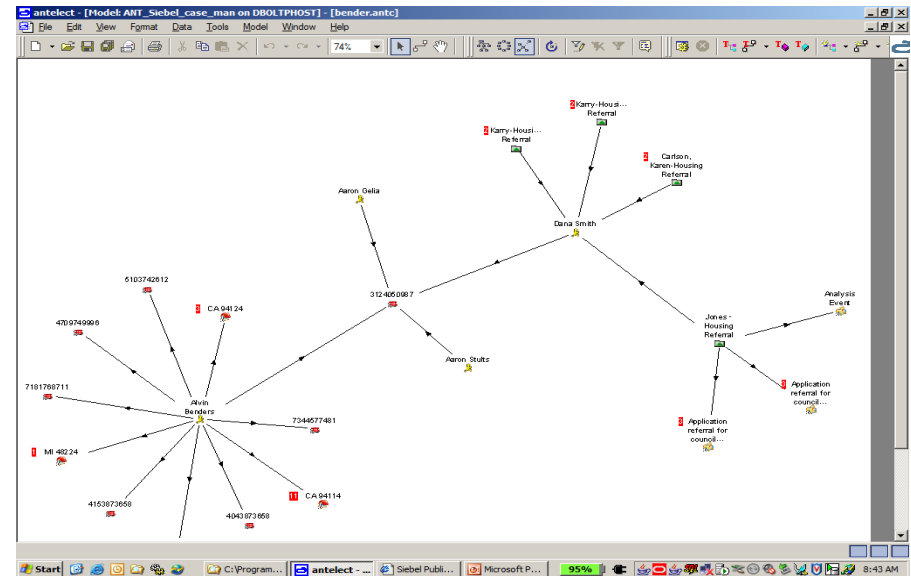
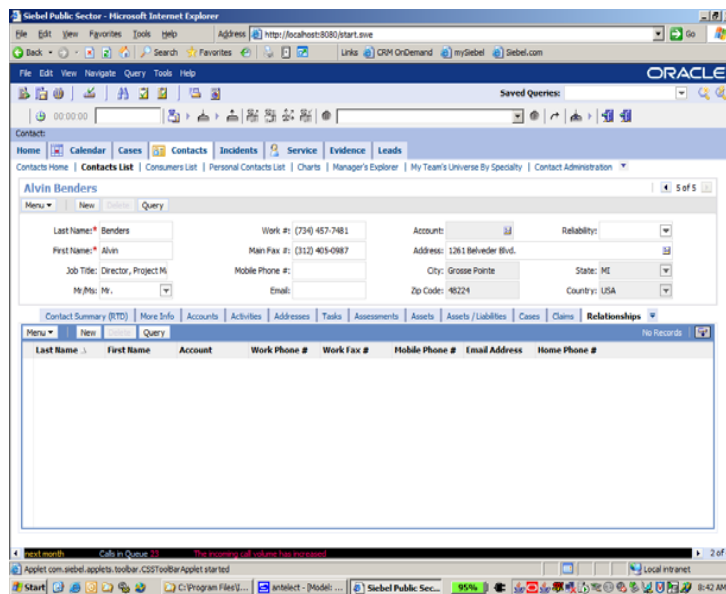
# Active Intelligence Hub



- Command & Control Center for Monitoring
  - Terrorism (physical and cyber)
  - Crisis
  - Natural disaster response
  - International criminal networks
  - Major Events
- Increasing demand for:
  - Real-time intelligence
  - Trusted information sharing
  - Rapid integration of disparate data
  - Response agility
  - Fast, reliable innovative solutions

# Visualisation Integration

“Visual Search Displays the links between people, vehicles, locations, phones and a wide range of other entities, allowing investigators or frontline operatives to see the patterns in their data and progress investigations or assessments more effectively”



ORACLE

# Visualise the Person

The screenshot displays the Oracle CRM Visualize interface. At the top, there is a navigation bar with tabs for Home, Calendar, Cases, Contacts, Incidents, Service, Evidence, and Leads. Below this, a contact profile for Gerald McCann is shown with fields for Last Name, First Name, Work #, Main Fax #, Mobile Phone #, Email, Account, Address, City, State, Zip Code, Reliability, and Country. The contact is associated with the 'Wire Imports' account and has a reliability of 'Unknown'. The address is '9 South Street, Chelsea, SW1 3JA, UK'. Below the profile, a 'Visualize' section shows a network diagram with 'Gerald McCann' at the center. The diagram includes nodes for 'Photographing Angel Tube station', '0208 1234567', '0780 2345678', 'Graham Green', 'NW2 7GF', '0207 123 4567', 'Wire Imports', 'Hydrogen Peroxide - Large Purchase Attempt', and 'SW1 3JA'. A status bar at the bottom indicates 'The incoming call volume has increased'.

# Information linked to an Address

The screenshot displays the Oracle CRM interface for a contact named Gerald McCann. The contact details form includes:

- Last Name: \*McCann
- First Name: \*Gerald
- Job Title: (empty)
- Mr/Ms: Mr.
- Work #: +4402071234567
- Main Fax #: (empty)
- Mobile Phone #: (empty)
- Email: (empty)
- Account: Wire Imports
- Reliability: Unknown
- Address: 9 South Street
- City: Chelsea
- State: (empty)
- Zip Code: SW1 3JA
- Country: UK

The 'Visualize' tab is active, showing a network diagram with the following nodes and connections:

- Red Flying Saucer** (UFO icon) is connected to **Allen Anderson** (person icon) and **Anouar Ane** (person icon).
- Europe Air Cargo** (airplane icon) is connected to **Allen Anderson**, **Anouar Ane**, and **Graham Brand** (person icon).
- Graham Brand** is connected to **SW1 3JA** (house icon).
- SW1 3JA** is connected to **Gerald McCann** (person icon).
- Allen Anderson** is connected to **0208 1234567** (phone icon).
- Anouar Ane** is connected to **0208 1234567** and **Photographing Angel Tube station** (lightbulb icon).
- Photographing Angel Tube station** is connected to **Gerald McCann**.
- Gerald McCann** is connected to **0780 2345678** (phone icon) and **00** (phone icon).

The interface also shows a top navigation bar with 'ORACLE' and 'Saved Queries', and a bottom status bar with system messages like 'Oldest Call Waiting 2:23' and 'Open enrollment for all company benefits begins next month'.

# Information Linked to a Phone

The screenshot displays the Oracle CRM interface. At the top, the Oracle logo is visible. Below it, a navigation bar includes tabs for Home, Calendar, Cases, Contacts, Incidents, Service, Evidence, and Leads. The main content area shows a contact record for Gerald McCann with the following details:

- Last Name: \*McCann
- First Name: \*Gerald
- Job Title: (empty)
- Mr/Ms: Mr.
- Work #: +4402071234567
- Main Fax #: (empty)
- Mobile Phone #: (empty)
- Email: (empty)
- Account: Wire Imports
- Reliability: Unknown
- Address: 9 South Street
- City: Chelsea
- State: (empty)
- Zip Code: SW1 3JA
- Country: UK

Below the contact record, a 'Visualize' section shows a network diagram. The central node is Gerald McCann, represented by a person icon. He is connected to several other nodes:

- Europe Air Cargo (building icon)
- Photographing Angel Tube station (lightbulb icon)
- 0780 2345678 (phone icon)
- Graham Green (person icon)
- NW2 7GF (building icon)
- Graham Brand (person icon)
- Ashvik Khan (person icon)
- SW1 3JA (building icon)
- 0208 1234567 (phone icon)
- Kaden Sa Laad (person icon)
- Allen Anderson (person icon)
- Anouar Ane (person icon)

The diagram uses various colored lines (blue, red, green, purple) to represent different types of relationships between the central contact and the other entities.



# Value Proposition for Customer

- ✓ Enables integration of information intelligence and incident data
- ✓ Increases efficiency of criminal investigation process
- ✓ Enhances collaboration of confidential info. securely across organisation
- ✓ Focus on real threats or issues
- ✓ Enables Business Intelligence, Crime Trend Analytics, Proactive Policing, & Resource optimisation
- ✓ Embeds intelligence into business process
- ✓ Minimises admin. time & maximises patrol time for front line officers (mobility)
- ✓ Can replace several business critical applications for Law Enforcement to save \$Ms in recurrent expenditure.
  - ✓ Incident Management (RMS)
  - ✓ Investigative Case Management
  - ✓ Property & Seized Forensics Evidence Management
  - ✓ Analytics that provide Crime Trends and Statistics

