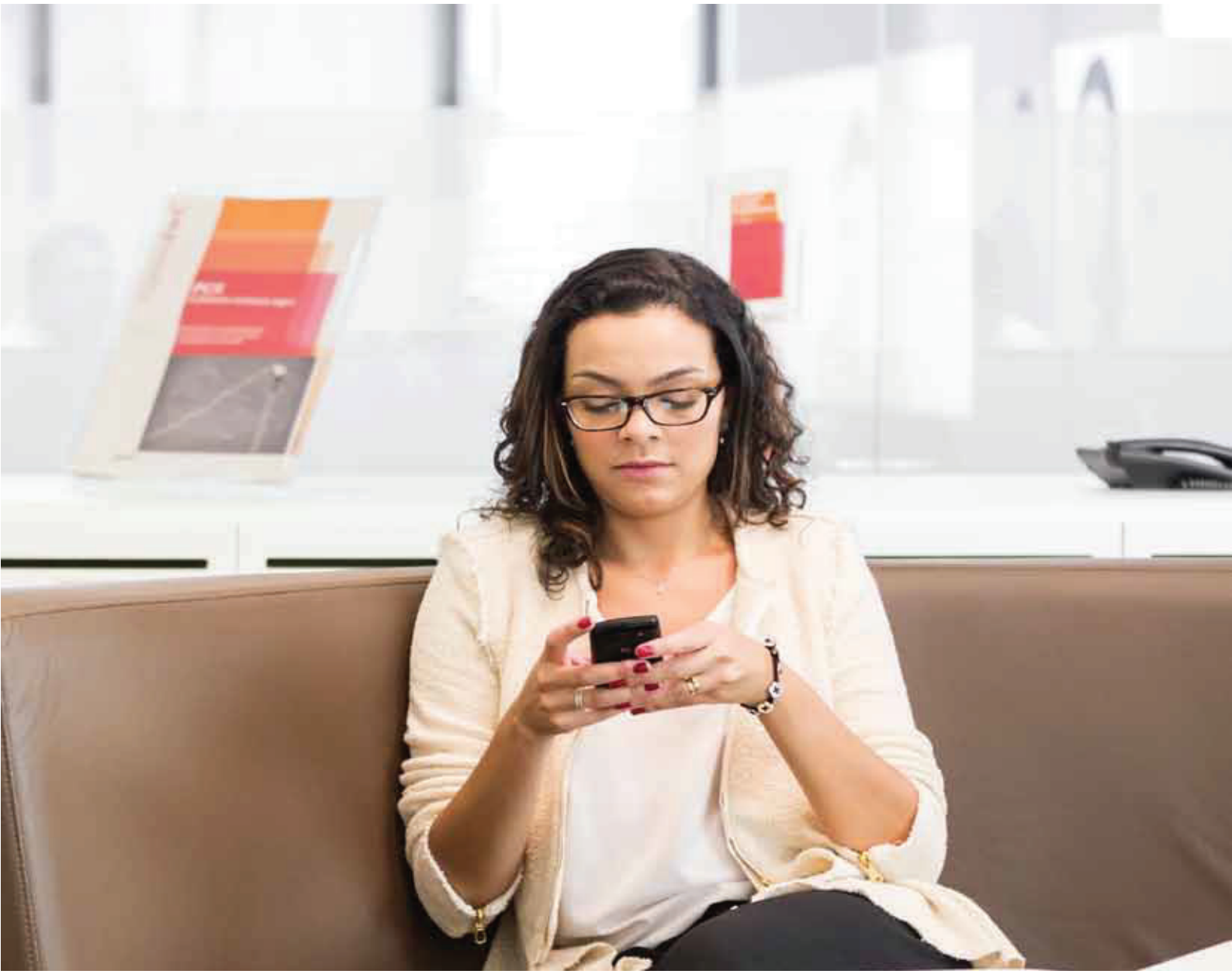
Forensic services
Telecommunications

pwc

Are you facing any of the following challenges?

- High usage frauds
- Vishing frauds
- Procurement and contracts related frauds
- Premium rate services (PRS) related frauds
- Fraudulent billing and waivers
- Money laundering, through m-commerce
- Unauthorised activations and adjustments to subscriber profile
- Commission arbitrage and misuse of promotions
- Misuse of internal and test SIM cards
- Disputes between telecom service providers and their business partners
- Other accounting/complex technical frauds

PwC's Forensic Telecom team can help you address these and many more....



*20,000+ man hours of investigations in telecom domain**

Dedicated forensic telecom practice, part of 350+ strong forensic team

Fully integrated capabilities in India for telecom fraud analytics

Experience in investigation of complex technical frauds

Experience of working with regulators

** Telecom operators, passive infrastructure providers, telecom equipment vendors and value added services (VAS) providers*

What differentiates us

Ensuring the best quality in whatever we do is the foundation of our value system. PwC India's Forensic Telecom team has experienced professionals to steer you through your concerns.

- ***50+ years*** combined work experience of leadership team with telecom clients
- Multi-disciplinary professionals comprising ***telecom engineers, forensic accountants, certified fraud examiners, MBAs, former police officers, lawyers, information technology experts***, with adept knowledge of the sector
- Dedicated on-site, state-of-the-art forensic labs with high-end servers capable of processing voluminous data, with storage capacity ***over 100 terra bytes***

Our offerings

Fraud management strategy

We help telecom companies develop and implement an entity-wide fraud management strategy with focus on three objectives – prevention, detection and response to fraud risks.

Traditionally, Telcos have battled frauds in silos of revenue assurance, IT security, corporate vigilance, etc. A comprehensive and integrated fraud management strategy enables Telcos to avoid duplication of effort, resource fragmentation, slipping through the cracks and provides 'one view' of fraud risks and potential perpetrators. Our in-depth knowledge of industry best practices can help you leapfrog to develop a best-in-class anti-fraud framework.

An integrated fraud management strategy encompasses the following:

Prevention: Assessment and strengthening of telecom organisations' ethics framework and processes, prevention primarily includes review of code of conduct, whistleblower policies, incident response mechanism and entity and process level fraud risks, etc.

This leads to an alignment of the ethics framework and detailed mapping of preventive and detective controls to manage fraud risks.

Detection: This includes review of the existing policy and processes for fraud detection and setting up a comprehensive fraud detection framework.

Response: This includes a streamlined, speedy and structured mechanism to respond to fraud incidents. This will include assessment of various in-sourced, co-sourced and out-sourced models.

Telecom fraud analytics

Telecom fraud analytics is used for a high degree of automation and generation of transaction alerts based on identified fraud risk scenarios for proactive monitoring. It helps Telcos discover anomalous patterns of emerging fraudulent behaviours and proactively identifying red flags across voice, data, SMS and other value-added services.

Our specialised skills to perform social networking analysis and investigative data linking such as CDR analysis, users/IMEI correlation analysis, unconventional IMSI/IMEI utilisation, etc. on voluminous data helps us uncover the relationship among users, phones and identify perpetrator(s) in investigations as well.

Fraud and misconduct investigation

Our team can conduct event-led investigations by gathering and analysing data to help identify instances of impropriety, the parties involved as well as uncover the modus operandi. We also follow the approach to gather and protect evidence that can be presented in a court of law, provide expert witness services and provide litigation support.

Incident response management service

Our domain specialised skills can help you handle sporadic incidences, find out the modus operandi, repeat offenders as well as gaps in key process, thereby enabling a quick turnaround for avenues such as incidence resolution and mitigating revenue, and reputation loss.

Fraud control unit set-up

Our practice has assisted companies in setting up fraud control units (FCUs) on a design-build-operate-transfer model. We have helped design the governance and operational framework of the FCU, data analytics based queries for processes and functions that are monitored as part of the FCU. We adopt an all-encompassing approach, analysing all the applications and their data, irrespective of whether they have existing interfaces, as well as data from external sources such as credit bureaus and social networks.

Fraud management system (FMS) set-up and effectiveness

We assist telecom companies to effectively implement and utilise fraud management systems, thus enabling appropriate return on its investment. We offer the following services:

- End-to-end support during implementation of fraud management framework
- Periodic reviews to ensure appropriate calibration of the framework
- Help in operating the fraud management system on a day-to-day basis, either from the office premises or offshore

Fraudulent activity reporting service

We can help you with threats and discussions prevailing on social media, websites as well as other content through our subscription services. You can get an edge over perpetrators by obtaining an outsider's view of fraudulent activities targeted at your company and supplement inward focus on fraud management.

Fraud risk review for IT and network systems

We assist companies in developing strategies to handle the end-to-end information lifecycle, right from creation to destruction of confidential information. Our specialised Forensic Technology Services practice assists companies in

- Managing access to digital assets
- Investigating incidents related to cyber crime such as intellectual property theft
- Unauthorised access to digital assets, changes to database and critical system configuration, phishing attacks
- Denial of service attacks
- Website defacement
- Malware analysis
- Any other unauthorised activity on the network through the use of forensic analytics
- E-discovery procedures, etc.

We can also review your company's existing policies related to identity and access management, firewalls, host intrusion detection and prevention, anti-virus and malware, data backups and system management server.

Telecom contract reviews

Telcos have outsourced critical business processes and have large and long duration service contracts with network vendors, IT providers, contact centre providers, etc.

We help review these contracts for the following:

- Recover revenues
- Identify unapplied penalties
- Identify missed service level agreements (SLAs) leading to potential cost savings
- Detect misapplied payment terms
- Identify vague and un-implementable contract clauses for rectification
- Recommend event and reporting controls to strengthen contract management

Corporate intelligence

Beyond background checks, our corporate intelligence practice evaluates the integrity, reputation as well as the performance track record of individuals, management groups, and corporate entities. This is done by collecting and analysing information that provides crucial insights for business decision-making. This practice can also gauge a wide spectrum of potential risks for companies seeking to enter an emerging market for the first time.

Dispute advisory services

Our specialists deliver a wide range of services to help prevent and resolve disputes and other forms of disagreements within business arrangements. We provide assistance in the analysis of issues, evidence collation, evaluation of damage arising from a breach and expert witness testimony in arbitration, mediation, transaction disputes and insurance claims.

Our forensic telecom team has experience with various fraud scenarios

Case study 1: Subscription and provisioning fraud

Scenario: Setting up a false identity to gain access to network services and use it without incurring charges

Fraudulent subscriber obtains post-paid connections with limited services	Accomplice (employee at service provider) provisions high-value services (ISD, PRS, roaming, etc.)	SIM card shipped to various destinations and no payments made for its usage	Fraudster benefits as a user or as an operator partner (PRS, content, interconnect, etc.)
Root cause			
• Violation of KYC norms • Inadequate customer verification checks	• Sharing access credentials • Inadequate background check	• Absence of a subscriber and services reconciliation • Fraudulent PRS numbers not tracked or blocked	• Delay in high usage reporting between operators
Solution			
Identify control gaps in the KYC norms subscriber verification processes.	Monitor and analyse user activity and access control logs.	Review FMS rules and ensure adequacy.	Conduct subscriber and services reconciliation, and implement a mechanism to block unauthorised services.

Case study 2: Unauthorised network configuration changes in a carrier network operator

Scenario: Configuration changes in the VoIP firewall of the carrier network to enable unauthorised VoIP traffic

Calls originating from other countries	Increased billing disputes with international VoIP carriers	Calls destined within the country
Root cause		
Modifications to the network firewall, through telnet allowing unauthorised incoming VoIP calls	Perpetrator added the range of unauthorised IP addresses in the rule and mapped the same to one of the international carriers	Due to masking, it appeared that the traffic was originating from one of the authorised international carriers
Solution		
IP tracing and the log analysis revealed that the source IP addresses of such unauthorised changes belonged to an overseas operator.	Several control gaps in access controls, security architecture and log management were observed in the operator's network.	Modify the control framework design to mitigate risks related to the above.

Case study 3: Misconduct in international long distance (ILD) services of a Telco

Scenario: Providing favourable voice call termination rates to ILD carriers with vested interest, causing revenue loss to the Telco

Telco (ILD business) executes agreement with preferential commercial terms with a Tier 3 ILD carrier for international calls termination in India.	Unusual discount is offered on call termination tariff to specific Tier 3 ILD carrier despite low incoming call traffic, causing revenue loss to the Telco.	Target and accomplice from ILD business had direct vested interest in the suspected Tier 3 ILD carrier.
Root cause		
• Lack of segregation of duties (SOD) in the Tier 3 ILD carrier on-boarding process • Absence of policy document for classification of tier-wise ILD carriers for finalising commercial terms	• Lack of defined parameters (business case) for offering discounted termination rates • No defined exception approval process with authority matrix	• Absence of defined process to conduct background checks on ILD carriers while on-boarding, to identify any conflict of interest
Solution		
Telco to put in place a SOD matrix defining roles and responsibilities during carrier on-boarding and a policy defining criteria for classification of tier-wise carriers.	Proper business case to be documented and approved when a rate lower than the base or floor rate is offered to a new ILD carrier.	An independent department or process to conduct background checks to identify and restrict on-boarding of related and blacklisted ILD carriers.

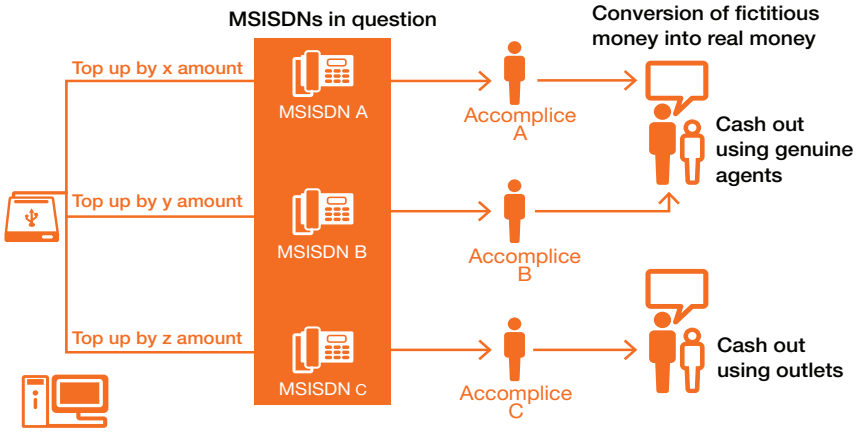
Case study 4: Generation of fraudulent m-commerce balances

Scenario: Fraudulent balance created in the m-commerce account, and subsequently transferred or cashed

Unexplained differences were found in e-value balances between the end-of-day cash balance on the m-commerce platform and the daily cash report.

- Review of system logs and audit trails uncovered multiple incidents of unauthorised access and updates to the m-commerce database
- MSISDNs' e-value balances were manually updated (topped up, topped down or both).

Investigation found that the perpetrator remotely connected to the network through 'toad' and made unauthorised updates to the m-commerce platform.



Perpetrator accesses m-commerce database system, approves MSISDN registrations and tops up e-value balances of the same (fictitious money).

Perpetrators cashed balances through unsuspecting agents

Case study 5: Misuse of m-commerce promotional scheme

Scenario: Promotional offer for additional credit on recharge amount misused by sales channels

Sales channel Fraudulent subscribers

- Retailer activates numerous connections, using unsuspecting subscriber documents (such as proof of identity, address, etc.)
- Use of cross-documentation between operators to evade the de-duping process
- Subscribes to m-commerce through the fraudulently activated connections
- Recharges the m-commerce accounts
- Retailer spends the m-commerce amount through various payment channels

Solution

- Stringent internal process for compliance with KYC norms for subscriber sign-up
- Proactive monitoring of retailer activities, especially during the promotional offers
- Periodically update blacklists (merchant, distributor, retailer and subscribers)
- Effective claw back clause for the retailer commission pay-out
- Proper service agreements and adequate security deposit wherever applicable

Example: Retailer earning

Commission for enrolling new subscribers for telecom services: 5 USD per subscriber	5 USD x 1,000 subscribers = 5,000 USD
Commission for enrolling new subscribers for m-commerce: 2 USD per subscriber	2 USD x 1,000 subscribers = 2,000 USD
One per cent commission on m-commerce recharges: 100 USD per subscriber	100 USD x 1% x 1,000 subscribers = 1,000 USD
Promotional offer benefit at the rate of 2% on recharges: 100 USD per recharge	100 USD x 2% x 1000 subscribers = 2,000 USD

In total the retailer earns 10,000 USD

Case study 6: Dispute resolution for a leading passive infrastructure provider

Scenario: A leading passive infrastructure provider involved in a dispute with another telecom firm to whom the passive infrastructure was leased

Comprehensive assessment of the terms and conditions of the contracts

Sample testing to analyse veracity of claims and deductions by both the parties

Successfully devising a mechanism to settle the dispute pertaining to areas of infrastructure provisioning, outage penalty, power and fuel expenses, maintenance costs, and deduction claims agreed by both the parties

About PwC

PwC helps organisations and individuals create the value they're looking for. We're a network of firms in 157 countries with more than 195,000 people who are committed to delivering quality in Assurance, Tax and Advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com.

In India, PwC has offices in these cities: Ahmedabad, Bangalore, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.in

PwC refers to the PwC network and / or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

You can connect with us on:

facebook.com/PwCIndia

twitter.com/PwC_IN

linkedin.com/company/pwc-india

youtube.com/pwc

Contact us

Arpita Pal Agrawal
Global Leader, Forensic Telecom Services
Mobile: +91 9811156161
Fixed line: +91 (124) - 3306003
Email: arpita.p.agrawal@in.pwc.com
PricewaterhouseCoopers Private limited
Building 10-C, 17th floor, DLF Cyber City
Gurgaon 122002, India

pwc.in

Data Classification: DC0

This publication does not constitute professional advice. The information in this publication has been obtained or derived from sources believed by PricewaterhouseCoopers Private Limited (PwCPL) to be reliable but PwCPL does not represent that this information is accurate or complete. Any opinions or estimates contained in this publication represent the judgment of PwCPL at this time and are subject to change without notice. Readers of this publication are advised to seek their own professional advice before taking any course of action or decision, for which they are entirely responsible, based on the contents of this publication. PwCPL neither accepts or assumes any responsibility or liability to any reader of this publication in respect of the information contained within it or for any decisions readers may take or decide not to or fail to take.

© 2015 PricewaterhouseCoopers Private Limited. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers Private Limited (a limited liability company in India having Corporate Identity Number or CIN : U74140WB1983PTC036093), which is a member firm of PricewaterhouseCoopers International Limited (PwCIL), each member firm of which is a separate legal entity.

PD 370 - May 2015 Forensic services-Telecommunications flyer.indd
Designed by Corporate Communications, India