JUPITER PRIME
Consulting • Training • Advisory
جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Account Takeover and Mobile Banking Fraud Evidence Training Course

31 January – 4 February 2027
Cairo

Account Takeover and Mobile Banking Fraud Evidence Training Course

Ref: 2408_90582 **Date:** 31 January – 4 February 2027 **Location:** Cairo **Fees:** 3500 GBP

Account Takeover and Mobile Banking Fraud Evidence is a 1-week training course for bank fraud and financial crime investigators who must prove how app or online access was hijacked, building a digital evidence case file. As fraud shifts to stolen credentials, SIM swaps and social engineering, banks need investigators who read device and session traces quickly. Jupiter Prime Training delivers this Account Takeover and Mobile Banking Fraud Evidence course.

Why Account Takeover and Mobile Banking Fraud Evidence Matters Now

Three forces shape this work. Customers bank mainly through apps, so decisive traces sit in session logs and device identifiers rather than branch paperwork. Criminal groups combine phishing, malware and mule accounts, moving funds within minutes. And courts and complaint bodies increasingly question whether a disputed payment was authorised. A bank that preserves this evidence well recovers funds and defends refund decisions; one that handles it badly loses cases. The course rests on recognised digital evidence handling principles: integrity, chain of custody, repeatability and proportionate collection.

Who Gains Most from Account Takeover and Mobile Banking Fraud Evidence

- Investigators handling disputed online transfers.
- Analysts extracting session and device records from banking platforms.
- Case handlers coordinating with telecom providers and law enforcement.
- Specialists examining customer handsets, emails and messages.
- Reviewers deciding refund liability for legal counsel.

Fraud units gain most when an investigator, a log analyst and a case reviewer attend together and agree one evidence standard.

Account Takeover and Mobile Banking Fraud Evidence Capabilities

Participants move from a complaint to a reconstructed record of who logged in, from which device, and where the money went:

- Map credential theft, SIM swap and remote access attack paths — for case triage.
- Extract login, session and device fingerprint records without altering them — for evidence integrity.
- Build an event timeline across app, call centre and payment logs — for authorisation disputes.
- Assess handset, email and message evidence — for weighing customer claims.
- Specify chain of custody records and hash values for every exhibit — for legal counsel and courts.
- Communicate findings in a case narrative — for refund panels and police referral.

Key Account Takeover and Mobile Banking Fraud Evidence Terms

- Account takeover — Fraud in which a criminal controls a genuine customer's app or online banking access and moves funds.
- SIM swap — Transfer of a victim's mobile number to a criminal's SIM card to intercept one-time passcodes.
- Device fingerprint — Hardware and software attributes identifying the handset or browser used in a session.
- Session log — Platform record of each login, action and network address in one banking session.
- Chain of custody — Record of who collected, held or examined an exhibit, and when.
- Hash value — Digital fingerprint of a file showing an exported record has not changed.

Account Takeover and Mobile Banking Fraud Evidence Day by Day

Day 1: How Accounts Are Taken Over

- Credential Phishing and Fake Banking Apps — Recognising the Entry Point
- SIM Swap and Passcode Interception — Telecom Evidence Worth Requesting
- Remote Access and Impersonation Scams — Authorised Versus Unauthorised Payments
- Mule Account Networks — Following Funds Beyond the First Hop
- Case Triage Matrix — Deciding Which Complaints Need Full Investigation

Day 2: Platform and Transaction Log Evidence

- Login and Authentication Records — Proving Who Passed Each Security Step
- Device Fingerprint and Network Address Data — Linking Sessions to Handsets
- Beneficiary Changes and Limit Increases — Spotting the Takeover Moment
- Payment Message and Core Ledger Trails — Matching Logs to Money Movement
- Read-Only Export and Hashing — Preserving Records Without Alteration

Day 3: Mobile Device and Email Evidence

- Customer Handset Examination Consent — Scope, Privacy and Proportionality Limits
- Installed App and Permission Review — Detecting Remote Access Tools
- SMS, Call and Messaging History — Corroborating Social Engineering Claims
- Email Header Analysis — Tracing Phishing Messages to Their Source
- Screenshot and Photo Evidence Limits — Weighing Material Customers Supply

Day 4: Building Proof and Decisions

- Unified Event Timeline — Reconciling App, Call Centre and Payment Times
- Chain of Custody Register — Recording Every Exhibit Handover
- Authorisation Liability Assessment — Customer Negligence Versus Bank Control Failure
- Production Orders and Third-Party Requests — Telecom and Receiving Bank Records
- Investigator Witness Statement — Presenting Technical Findings in Plain Language

Day 5: Practising the Digital Evidence Case File

- SIM Swap Case — Applying Log Extraction and Timeline Reconstruction
- Insurance Customer Phishing Case — Testing Email and Handset Evidence
- Mule Network Exercise — Linking Device Fingerprints Across Accounts
- Peer Challenge of Exhibits — Spotting Gaps a Defence Would Exploit
- Digital Evidence Case File — Final Assembly for Legal Review

Applying Account Takeover and Mobile Banking Fraud Evidence After the Course

- Reopen a recent account takeover complaint, rebuild its timeline from session and device records, and compare it with the original decision.
- Draft a one-page read-only export and hashing procedure for platform logs with the platform owner.

Account Takeover and Mobile Banking Fraud Evidence Questions FAQ

What is account takeover and mobile banking fraud evidence, and why does it matter now?

It is the digital proof of how a customer's banking access was hijacked. It matters now because most disputed payments begin in an app, and refund and prosecution decisions depend on session, device and telecom records.

Which roles gain most from account takeover and mobile banking fraud evidence skills?

Fraud investigators and log analysts gain most. Case reviewers deciding refund liability, and staff liaising with telecom providers and law enforcement, also benefit.

How does account takeover and mobile banking fraud evidence differ from a forensic accounting course?

It focuses on digital channel traces rather than accounting records. Forensic accounting examines ledgers and statements, while this subject reconstructs the logins, devices and messages behind one compromised account.

What do you bring back from account takeover and mobile banking fraud evidence training?

You bring back a case file built on a realistic case: triage record, hashed log extracts, event timeline, custody register and liability assessment.

Account Takeover and Mobile Banking Fraud Evidence: The Way Forward

The digital evidence case file gives a head of fraud investigations the first decision it informs: whether a disputed payment was authorised and who bears the loss. Investigators, legal counsel and recovery teams use it as one shared record. After its first use, the export and custody steps are worth revisiting, since platform log formats and fraud methods change often.