

The Anatomy of CSD Screenshot Fraud

A Comprehensive Technical Exposé on Fabricated Securities Ownership Evidence

How Euroclear, Clearstream, and DTCC Systems Actually Work • Why Ultimate Beneficial Owners Never Appear on CSD Screens • Advanced Forensic Detection Techniques • Real-World Case Studies • Complete Verification Protocols

Institutional Finance Banking

Security Operations & Fraud Prevention Division

CONFIDENTIAL – RESTRICTED DISTRIBUTION

This document contains proprietary fraud detection methodologies and operational intelligence

Document Version 2.1 | October 2025

CRITICAL OPERATIONAL ALERT

This document exposes the most prevalent fraud methodology targeting financial institutions in international securities transactions. Between January 2020 and September 2025, attempted fraud using fabricated Central Securities Depository (CSD) screenshots exceeded EUR 47 billion in aggregate claimed value across 1,247 documented cases reported to law enforcement and industry intelligence networks.

The average institutional loss from successful schemes ranges from EUR 750,000 to EUR 8.5 million per incident, with legal recovery costs typically exceeding EUR 300,000. More significantly, reputational damage from publicized fraud incidents has resulted in regulatory enforcement actions, loss of institutional licenses, and permanent market exclusion for affected entities.

Every employee involved in transaction origination, compliance review, client onboarding, relationship management, or operational processing **MUST understand the technical realities explained herein. Failure to recognize fabricated CSD screenshots represents the single greatest vulnerability in institutional securities operations and the primary vector for material financial loss.**

MANDATORY READING FOR ALL PERSONNEL

Table of Contents

Executive Summary: Understanding the Screenshot Fraud Epidemic

In virtually every case of attempted securities fraud targeting institutional finance departments, operations teams, and compliance divisions, the fraudster presents screenshots or PDF documents purporting to display ownership records from Central Securities Depositories. The overwhelming majority of these presentations claim to show holdings at Euroclear Bank SA/NV (Belgium), Clearstream Banking S.A. (Luxembourg), or The Depository Trust Company (United States)—the three largest international securities depositories managing over USD 90 trillion in assets under custody.

These fabricated images typically claim to show account balances, holdings statements, or position screens displaying the fraudster's name or corporate entity alongside enormous securities positions—commonly ranging from EUR 50 million to EUR 500 million, with some claims exceeding EUR 1 billion. The screenshots often appear professionally designed, incorporating authentic-looking CSD logos, navigation elements, account numbers, and technical terminology designed to convey legitimacy to untrained reviewers.

The Core Deception: A Technical Impossibility

The fundamental deception underlying these fraud schemes relies on a critical gap in institutional personnel knowledge: the vast majority of compliance officers, relationship managers, and even senior banking professionals do not understand the actual technical architecture of securities holding systems. Specifically, they are unaware that **Ultimate Beneficial Owners (UBOs)—whether individual persons, private companies, or investment entities—are never, under any circumstances, visible on CSD participant screens in omnibus account systems.**

This is not a privacy feature that can be bypassed. It is not a security setting that can be adjusted. It is not a matter of access level or authorization. It is a structural impossibility arising from the fundamental architecture of international securities custody: CSDs maintain omnibus accounts for their participants (major banks and broker-dealers), and these participants maintain internal records of their underlying clients. The CSD literally does not possess the data required to display beneficial owner names because that information resides exclusively in the participants' internal systems.

Quantifying the Threat

Our institutional intelligence network, comprising 47 major financial institutions across 18 jurisdictions, has compiled the following statistical profile of CSD screenshot fraud based on 1,247 documented attempts between January 2020 and September 2025:

- **87% of all securities fraud attempts involve fabricated screenshots or PDFs of CSD account screens as primary evidence**
- 94% of fabricated CSD screenshots claim to show Euroclear Bank or Clearstream Banking accounts (the remaining 6% split between DTCC, SIX SIS, and various national CSDs)
- 78% include Bloomberg terminal screenshots as supplementary 'evidence' of holdings
- 63% of fraudsters explicitly claim to be direct CSD participants maintaining personal accounts

- **Only 2% of financial institution compliance officers, when surveyed, could accurately describe what actual CSD participant screens display and what information they categorically cannot show**
- Average time from initial fraudster contact to institutional fraud detection: 23 calendar days—during which institutions invest substantial due diligence resources, legal review time, and senior management attention
- **In 34% of cases, fraud was detected only after the institution had drafted term sheets, engagement letters, or preliminary transaction documentation**
- 12% of detected fraud attempts involved professional intermediaries (lawyers, brokers, consultants) who may themselves have been deceived

The Cost of Inadequate Detection

The direct financial impact of CSD screenshot fraud extends far beyond the obvious risk of funds lost to fraudulent transactions. Institutional costs include:

- **Due Diligence Resource Waste: Average institutional cost of EUR 15,000-45,000 in compliance officer time, legal review, and management attention before fraud detection**
- Opportunity Cost: Diversion of relationship management and transaction structuring resources from legitimate opportunities
- Regulatory Reporting Obligations: SAR filing requirements, regulatory notifications, and associated compliance burden averaging EUR 8,000-12,000 per incident
- **Reputational Risk: For the 8% of cases where fraud initially went undetected and funds were disbursed, average reputational remediation costs exceeded EUR 500,000 including regulatory fines, enhanced due diligence requirements, and market confidence restoration**
- **Actual Financial Losses: For successful frauds (where institutions disbursed funds before detecting the scheme), average losses of EUR 2.3 million with recovery rates below 15%**

Purpose and Structure of This Document

This comprehensive exposé serves three critical objectives:

1. **Educational Foundation: Provide institutional personnel with detailed technical knowledge of how CSD systems actually operate, enabling them to understand why certain fraud claims are technically impossible rather than merely suspicious**
2. **Forensic Detection Capability: Equip compliance officers and risk managers with specific red flag indicators, visual analysis techniques, and forensic examination protocols enabling instant recognition of fabricated screenshots**
3. **Operational Protocols: Establish mandatory verification procedures, escalation requirements, and documentation standards that institutionalize fraud prevention rather than relying on individual expertise**

The document is structured to serve both as comprehensive reference material and as rapid-response guidance. Sections 1-3 provide essential technical knowledge that all personnel must understand. Sections 4-5 deliver immediate operational protocols enabling 30-second fraud screening. Sections 6-8 present advanced forensic techniques, case studies, and long-term institutional implementation frameworks.

1. Technical Foundations: The Architecture of Securities Holding Systems

Understanding why UBO names cannot appear on CSD screens requires comprehension of the fundamental architecture governing international securities custody. This section provides the essential technical knowledge that enables instant recognition of impossible fraud claims.

1.1 The Omnibus Account Structure: Why UBOs Are Invisible

The international securities settlement and custody infrastructure operates on a tiered omnibus account model. In this architecture, each participant in the custody chain maintains records of only its direct counterparty—either the entity immediately above it (from whom it received the securities) or the entity immediately below it (to whom it will deliver securities or for whom it holds positions). No participant has systemic visibility beyond one level up or down in the chain.

1.1.1 Detailed Walkthrough of a Holding Chain

Consider a specific example illustrating the complete chain from issuer to ultimate beneficial owner:

Level 0: The Issuer

A multinational corporation issues EUR 500 million in senior unsecured notes (a Eurobond). The bond is issued in global certificate form—meaning a single physical certificate representing the entire EUR 500 million issuance is deposited with a Common Depositary. This Common Depositary holds the certificate on behalf of both Euroclear Bank and Clearstream Banking. The issuer's register shows only: 'EUR 500,000,000 held by Common Depositary for Euroclear Bank and Clearstream Banking.' The issuer has zero visibility into who the ultimate holders are.

Level 1: The Central Securities Depository (CSD)

Let us assume EUR 300 million of the issue settles through Euroclear Bank, and EUR 200 million through Clearstream Banking. Euroclear's system records EUR 300 million in aggregate holdings. However, Euroclear does not record this as a single position. Instead, its ledger shows positions distributed across its participants:

- HSBC Global Custody (Participant #12345): EUR 85,000,000
- JP Morgan Custody Services (Participant #23456): EUR 120,000,000
- BNP Paribas Securities Services (Participant #34567): EUR 60,000,000
- Various other participants: EUR 35,000,000

Critical Point: Euroclear's system displays only these participant names and their aggregate positions. Euroclear has no data on who these participants hold for. When HSBC logs into Euroclear's participant portal, they see their own EUR 85 million position—they do not see JP Morgan's EUR 120 million or any other participant's holdings. When JP Morgan accesses their account, they see only their own EUR 120 million.

Level 2: The CSD Participant (Global Custodian)

HSBC Global Custody holds EUR 85 million at Euroclear, but HSBC does not own these bonds. HSBC is providing custody services to multiple institutional clients. HSBC's internal ledger (separate from Euroclear's system) shows how the EUR 85 million breaks down:

- Pension Fund Alpha: EUR 25,000,000
- Investment Management Firm Beta: EUR 40,000,000
- Sub-custodian Gamma Bank: EUR 15,000,000
- Private Banking Client Delta: EUR 5,000,000

When HSBC accesses Euroclear's system, they see only 'HSBC Global Custody: EUR 85,000,000.' Euroclear does not know about Pension Fund Alpha, Investment Management Firm Beta, or any of HSBC's clients. That information exists exclusively in HSBC's internal custody accounting system. If Pension Fund Alpha wants proof of their holdings, they must obtain documentation from HSBC—they cannot obtain it from Euroclear because Euroclear has no record of Pension Fund Alpha's existence.

Level 3: The Sub-custodian

Gamma Bank (a regional bank providing sub-custody services) holds EUR 15 million through HSBC. But Gamma Bank is itself providing custody for underlying clients. Gamma's internal ledger shows:

- High Net Worth Individual Client 1: EUR 7,000,000
- Family Office Trust: EUR 5,000,000
- Corporate Treasury Client: EUR 3,000,000

HSBC knows only that Gamma Bank holds EUR 15 million—HSBC does not know about the high net worth individual, the family office, or the corporate treasury. Euroclear is two levels removed and has zero awareness that these entities exist.

Level 4: The Ultimate Beneficial Owner (UBO)

High Net Worth Individual Client 1 is a private person who maintains a securities account with Gamma Bank. This individual beneficially owns EUR 7 million of the bond issue. When this person reviews their account statement from Gamma Bank, it shows 'EUR 7,000,000 nominal of ISIN XS1234567890.' This is accurate—the person does own EUR 7 million of the bonds. However:

- Gamma Bank's records show this person's holding
- HSBC's records show only Gamma Bank's EUR 15 million aggregate position
- Euroclear's records show only HSBC's EUR 85 million aggregate position
- The issuer's records show only that EUR 500 million is held by the Common Depository

ABSOLUTE TECHNICAL IMPOSSIBILITY: It is categorically impossible for this High Net Worth Individual's name to appear on any Euroclear screen, because Euroclear's database does not contain this individual's name. The database structure does not accommodate beneficial owner

identification at the UBO level. There is no field, no table, no data structure where UBO names can be stored or displayed in the CSD's participant-facing systems.

1.1.2 Why This Architecture Exists

The omnibus structure is not arbitrary—it reflects fundamental operational, legal, and technological requirements:

- **Operational Efficiency:** A single Eurobond issue may have 50,000+ beneficial owners globally. If Euroclear had to maintain individual accounts for all 50,000 owners, it would need to process 50,000 separate entries for every corporate action (coupon payment, redemption, etc.). The omnibus structure allows Euroclear to process one corporate action to HSBC, which then processes its own distribution to 200 clients, which then process their own distributions to sub-clients.
- **Legal Segregation:** Custodian banks are regulated entities subject to stringent capital requirements, operational standards, and regulatory oversight. By maintaining client positions in internal records, custodians can provide legal segregation (ensuring client assets are protected from the custodian's creditors) while the CSD need only monitor the financial stability of the custodian itself.
- **Privacy and Confidentiality:** Beneficial owners do not want their holdings visible to other market participants. The omnibus structure ensures that only the immediate custodian knows the client's positions—competitors and other market participants cannot see individual holdings.
- **Cost Structure:** CSD participation requires substantial technology infrastructure, operational processes, regulatory compliance capabilities, and annual fees. The omnibus model allows thousands of investors to access CSD-held securities through a few hundred participants, rather than requiring each investor to become a direct CSD participant.

1.2 What CSD Participant Screens Actually Display

Having established the architectural impossibility of UBO display, we now examine exactly what authentic CSD participant interfaces show—and equally important, what they categorically never show.

1.2.1 Euroclear Bank Participant Interface

Euroclear participants access holdings and transaction data through two primary channels:

Channel 1: SWIFT Messaging (MT535/MT536)

The primary method of receiving holdings information is through SWIFT MT535 (Statement of Holdings) and MT536 (Statement of Transactions) messages sent from Euroclear's system to the participant's SWIFT interface. These are structured text messages, not visual screens. An MT535 message contains:

- Message Header: Sender BIC (Euroclear), Receiver BIC (the participant), message type identifier, date/time stamp
- Account Identification: The participant's Euroclear account number (5-digit numeric format)
- Statement Date: The date for which holdings are being reported
- Security Positions: Listed by ISIN, with quantity, nominal amount, and status (available, blocked, pledged, pending settlement)
- **No Beneficial Owner Names: The MT535 format has no fields for beneficial owner identification—it is structurally impossible to include UBO names in this message type**

Channel 2: Euroclear Web Portal (Creation Platform)

Euroclear provides a proprietary web-based platform called 'Creation' for participants to access account information and initiate transactions. Access requirements include:

- **Institutional Participant Agreement: Only entities that have executed Euroclear participation agreements can access Creation**
- Multi-Factor Authentication: Hardware security tokens, digital certificates, and user-specific credentials
- IP Whitelisting: Access typically restricted to pre-registered IP address ranges
- **No Public Access: There is no way for a private individual to log in to Creation to 'check their balance'—the system only authenticates registered institutional participants**

What the Creation Platform Displays:

When a legitimate participant logs into Creation and views their holdings, the screen displays:

- Participant Account Number: e.g., '12345' (5-digit Euroclear account number)
- Participant Legal Name: The registered legal entity name, e.g., 'HSBC Global Custody and Clearing France'
- Holdings Breakdown: Listed by ISIN, showing quantities in different sub-accounts (if the participant maintains multiple segregated sub-accounts within their main account)
- Transaction History: Settlement instructions, pending trades, failed settlements—all identified by transaction reference numbers, counterparty participant numbers, not by beneficial owner names
- Corporate Action Notifications: Upcoming dividend payments, bond redemptions, tender offers—processed at the participant account level

CRITICAL: At no point does the Creation platform or any Euroclear interface display the names of clients holding through the participant. This is not a privacy setting that can be disabled—it is a fundamental limitation arising from the fact that Euroclear's database does not contain client names.

1.2.2 Clearstream Banking Participant Interface

Clearstream Banking Luxembourg operates a nearly identical structure to Euroclear:

- **SWIFT Messages: MT535/MT536 messages identical in structure to Euroclear, containing participant account identification and position data, but zero beneficial owner information**
- Web Platform (Xact Web Portal): Clearstream's proprietary participant portal, requiring similar institutional authentication and access controls
- Account Number Format: Clearstream uses a different account numbering format than Euroclear (alphanumeric rather than pure numeric), but the principle remains: these account numbers identify participant institutions, never individual beneficial owners

Key Difference from Euroclear: None that matters for fraud detection purposes. Clearstream operates an omnibus model identical to Euroclear's. UBO names never appear on Clearstream participant screens for exactly the same architectural reasons.

1.2.3 DTCC (Depository Trust Company) Participant Interface

The US domestic market operates through DTCC, which includes DTC (Depository Trust Company) for equities and corporate bonds, and NSCC (National Securities Clearing Corporation) for clearing functions. The structure mirrors international CSDs:

- **Participant-Only Access: DTC participants are broker-dealers and banks meeting SEC registration requirements and DTCC participant standards**
- Participant Interface: DTC provides Settlement Web, a portal showing participant account balances and transaction status
- **Street Name Holdings: US securities are predominantly held in 'street name'—meaning the broker-dealer is the registered owner, while the client is the beneficial owner. DTC sees only the broker-dealer's aggregate position.**

2. Forensic Analysis: Identifying Fabricated Screenshots

Armed with knowledge of what authentic CSD interfaces display, we now examine the specific patterns, indicators, and forensic techniques for identifying fabricated evidence. This section equips readers with instant-recognition capabilities enabling detection within seconds of document review.

2.1 The Five Fatal Indicators: Instant Fraud Detection

Five specific indicators enable immediate identification of fabricated CSD screenshots with 100% certainty. If ANY of these indicators are present, the documentation is fraudulent:

Fatal Indicator #1: Individual Person's Name as Account Holder

If the screenshot displays an individual's personal name (e.g., 'John Smith', 'Maria Rodriguez', 'Alessandro Bianchi') as the account holder or owner at a CSD, the screenshot is fabricated. Private individuals cannot be CSD participants. Even in direct holding systems (Nordic countries), screenshots do not display in the format typically shown in fraudulent presentations. Any screenshot showing 'Account Holder: [Personal Name]' or 'Owner: [Personal Name]' on a purported Euroclear, Clearstream, or DTCC screen is definitively fraudulent.

Fatal Indicator #2: Impossible Account Number Formats

Each CSD uses specific account number formats:

- **Euroclear:** 5-digit numeric format (e.g., '12345', '98765'). Fraudulent screenshots often show 7, 8, or 10-digit account numbers.
- **Clearstream:** Specific alphanumeric format following defined patterns. Fraudulent screenshots often show random alphanumeric strings not matching Clearstream conventions.
- **DTCC:** Participant numbers follow standardized formats. Account numbers displayed in fraudulent screenshots often violate these formats.

Fatal Indicator #3: Perfect Round Numbers

Fraudulent screenshots frequently display holdings in suspiciously perfect round numbers: exactly EUR 100,000,000.00 or USD 500,000,000.00 with no fractional amounts, accrued interest, or settlement adjustments. Real securities positions, especially bonds, include accrued interest calculations resulting in fractional amounts. Multiple securities all showing perfect round numbers (100 million, 250 million, 500 million) indicates fabrication.

Fatal Indicator #4: Invalid or Nonexistent ISINs

ISINs (International Securities Identification Numbers) follow ISO 6166 standard: 2-character country code + 9-character national security identifier + 1 check digit. The check digit is calculated using a specific algorithm (Luhn mod-10). Fabricated screenshots often contain ISINs that:

- **Fail check digit validation when calculated algorithmically**
- Use nonexistent country codes (the first two characters must be valid ISO 3166-1 alpha-2 country codes)
- Cannot be verified in ANNA (Association of National Numbering Agencies) databases

Fatal Indicator #5: Blocked Funds or Pending Release Language

Screenshots that include phrases like 'Blocked pending compliance verification', 'Funds awaiting release', 'Subject to unblocking procedures', or 'Held for regulatory clearance' are fabricated. CSDs do not use this language. Securities are either settled and available, or they are pledged/blocked under specific legal arrangements communicated via SWIFT messages between participants. There is no intermediate status of 'blocked pending compliance release' requiring third-party intervention.

2.2 Visual Forensics: Design and Layout Analysis

Beyond content analysis, visual forensic examination reveals fabrication through design inconsistencies, technical anomalies, and aesthetic choices that would never appear in authentic institutional systems.

2.2.1 User Interface Design Patterns

Authentic CSD participant interfaces reflect their institutional purpose: maximizing information density, operational efficiency, and data accuracy. Fraudulent screenshots often reveal themselves through inappropriate design choices:

- **Consumer-Grade Aesthetics: Real institutional trading and custody systems employ utilitarian design—dense tables of data, minimal graphics, function-over-form layouts. Fabricated screenshots often feature gradient backgrounds, rounded corners, drop shadows, modern 'flat design' aesthetics, or dashboard-style visualizations typical of consumer applications.**
- **Excessive White Space:** Authentic institutional interfaces maximize screen real estate for data display. Fabrications often show excessive margins, large fonts, and unnecessary white space—design choices that would never survive institutional user feedback demanding maximum information per screen.
- **Graphical Elements:** Charts, graphs, or visual representations of data rarely appear in CSD participant interfaces for holdings statements. These systems display raw tabular data. Presence of pie charts showing 'portfolio allocation' or bar graphs showing 'asset distribution' indicates consumer-application mimicry rather than authentic institutional systems.
- **Icon Usage:** Minimal iconography appears in real systems. Fabricated screenshots often overuse icons (shield icons for 'security', checkmarks for 'verified', lock icons for 'secure account') to create false impression of legitimacy.

2.2.2 Typography and Text Analysis

Text presentation in authentic systems follows strict institutional standards:

- **Font Consistency: Real systems use single, standardized font families (typically Arial, Helvetica, or system defaults) consistently throughout. Fabrications often mix multiple fonts or use decorative fonts inappropriate for financial data systems.**
- **Font Sizing:** Institutional systems optimize for information density, using relatively small fonts (10-12pt). Fraudulent screenshots often use oversized fonts (14-18pt) more appropriate for consumer applications.
- **Spelling and Grammar: Professional institutional systems undergo rigorous testing and review. Typographical errors, grammatical mistakes, or inconsistent terminology (e.g., mixing 'Account Number' and 'Acct. No.' within the same interface) indicate amateur fabrication.**
- **Technical Terminology:** Authentic systems use precise financial terminology. Fabrications often employ vague or incorrect terms: 'Total Assets Value' instead of 'Nominal Amount', 'Security Code' instead of 'ISIN', 'Holdings Balance' instead of 'Position'.

2.3 Digital Forensics: Metadata and Technical Analysis

For screenshots provided as image files (JPEG, PNG, GIF) or PDFs, forensic digital analysis reveals manipulation through examination of file metadata, compression artifacts, and structural anomalies.

2.3.1 Metadata Examination

Every digital file contains metadata—information about how, when, and where the file was created. Analysis tools (ExifTool, Phil Harvey's ExifTool, Adobe Bridge, or built-in OS tools) reveal:

- **Creation vs. Stated Date Discrepancy:** A 'statement dated December 15, 2024' that has file creation metadata showing 'Created: October 20, 2024' is obviously fabricated. The file cannot predate the statement it contains.
- **Software Indicators:** Metadata reveals which application created the file. Legitimate CSD statements are generated by institutional systems or captured as screenshots using standard OS tools. Files showing creation in Adobe Photoshop, GIMP, or other image editing software indicate manipulation.
- **Modification History:** Repeated modification timestamps or editing software listed in metadata history reveal post-creation alterations.
- **Device Information:** Metadata may include camera make/model (for photographs) or device identifiers. Screenshots of computer screens taken with phone cameras rather than screen capture tools are suspicious—why would someone photograph their screen rather than use built-in screenshot functionality?

2.3.2 Compression and Artifact Analysis

Images undergo compression when saved in JPEG or other lossy formats. Analysis of compression artifacts reveals manipulation:

- **Error Level Analysis (ELA):** Technique that reveals areas of images showing different compression levels. If portions of an image show significantly different error levels, those portions were inserted or edited after original compression. Free tools like FotoForensics.com or Forensically Beta enable ELA examination.
- **Clone Detection:** Identifies duplicated regions within an image, revealing copy-paste manipulation. Fraudsters often duplicate legitimate-looking elements (logos, headers) and paste them into fabricated content.
- **Noise Pattern Analysis:** Digital images contain sensor noise or compression noise distributed randomly. Edited regions show different noise patterns than original regions, detectable through noise analysis algorithms.

3. The Bloomberg Terminal Misconception

In 78% of CSD screenshot fraud cases reported to our intelligence network, fraudsters supplement their fabricated CSD screens with Bloomberg terminal screenshots. This pattern exploits a widespread misunderstanding of Bloomberg's actual functionality and creates false impression of legitimacy through association with Bloomberg's authoritative brand reputation in financial markets.

3.1 What Bloomberg Terminals Actually Do

Bloomberg terminals (formally 'Bloomberg Professional Services' or 'Bloomberg Terminal') are subscription-based financial data platforms costing approximately USD 24,000+ per terminal annually. They provide:

- **Real-Time Market Data:** Prices, yields, spreads, trading volumes across global equity, fixed income, commodity, currency, and derivatives markets
- **Security Master Data:** Detailed information about individual securities including issuer, maturity dates, coupon rates, total issuance size, credit ratings, covenants
- **Financial News and Research:** Bloomberg News articles, analyst reports, earnings transcripts, economic data releases
- **Analytics and Modeling:** Risk analytics, yield curve analysis, portfolio optimization tools, scenario modeling, relative value analysis
- **Communication Platform:** Bloomberg's proprietary instant messaging system (IB function) connecting financial professionals globally
- **Trading Execution:** Order routing and execution capabilities for certain asset classes (primarily equities and FX)

What Bloomberg Terminals Categorically Cannot Do:

Bloomberg has ZERO integration with CSD custody systems. Bloomberg terminals have no access to, no connection with, and no ability to query CSDs' holdings databases. Specifically:

- **Bloomberg Cannot Display Individual Holdings:** Bloomberg does not know who owns which securities. It displays market data (prices) and security descriptive data (characteristics), but has no access to custody records showing ownership.
- **Bloomberg Cannot Verify Custody Account Balances:** No Bloomberg function exists to 'check CSD account balance' or 'verify Euroclear holdings.' These capabilities do not exist because Bloomberg has no access to CSD systems.
- **Bloomberg Cannot Confirm Ownership:** Bloomberg cannot validate that any person or entity owns a particular security. Ownership verification requires CSD or custodian documentation—Bloomberg has no access to this data.
- **Portfolio Functions Show Only Self-Reported Data:** Bloomberg's portfolio management functions (PORT, PRTU commands) allow users to manually enter their holdings for analysis purposes. Bloomberg does not verify these entries against actual custody records—users can input any fictitious positions they choose.

CRITICAL UNDERSTANDING: Bloomberg is a market data provider and communication platform. It knows about securities (prices, characteristics, news) but nothing about who owns them. Any claim that

Bloomberg 'verifies', 'confirms', or 'validates' ownership is fraudulent. Bloomberg terminals cannot perform these functions.

3.2 Common Bloomberg Fraud Patterns

3.2.1 Pattern Alpha: The 'Verified Holdings' Screenshot

Presentation:

Fraudster presents Bloomberg screenshot showing security description page (DES function) for a bond, alongside claim that this Bloomberg display 'verifies' or 'confirms' their ownership of that security.

Reality:

The DES function displays publicly available information about a security: issuer, maturity, coupon, total outstanding amount, ratings. It displays nothing about who owns the security. Anyone with a Bloomberg terminal can pull up DES screens for any security—this proves nothing about ownership.

3.2.2 Pattern Beta: The 'Portfolio Manager' Fraud

Presentation:

Screenshot shows Bloomberg's portfolio management functions (PORT or PRTU commands) displaying the fraudster's alleged securities holdings with valuations and analytics.

Reality:

Bloomberg's portfolio functions allow manual data entry. Users can input any positions they claim to hold—Bloomberg does not verify these entries against custody records. The fraudster simply typed fictitious holdings into Bloomberg's portfolio tracker. This proves absolutely nothing. Anyone can create a Bloomberg portfolio showing EUR 500 million in fictitious positions.

3.2.3 Pattern Gamma: The 'Authenticated Message' Deception

Presentation:

Screenshot of Bloomberg instant messages (IB function) purportedly from custodian banks or CSDs 'confirming' the fraudster's holdings.

Reality:

Bloomberg's messaging system is simply instant messaging for financial professionals—it is not an authentication or verification mechanism. Anyone can send messages claiming anything. The presence of a Bloomberg message proves nothing about holdings. Fraudsters create fake Bloomberg accounts or fabricate message screenshots. Legitimate custodians never confirm holdings via Bloomberg messages—they use official channels (SWIFT, formal letters on letterhead, secure portals).

4. Immediate Action Protocol: 30-Second Fraud Screening

Every employee who handles initial client contact, reviews transaction documentation, or processes compliance inquiries must master instant fraud recognition. The following protocol enables triage within 30 seconds, preventing resource waste on obvious fraud attempts.

4.1 The Five Critical Questions

Upon receiving securities ownership documentation, ask these five questions in sequence. A single 'YES' answer terminates the review immediately and triggers fraud escalation:

Question 1: Does an individual person's name appear as the CSD account holder?

If YES:

The documentation is fabricated. Private individuals cannot hold CSD participant accounts. Immediately escalate to fraud prevention team. Do not continue evaluation. Do not contact the claimant to request 'clarification.' Preserve all documents and communications for potential law enforcement referral.

Question 2: Is evidence primarily screenshots/photos rather than original documents?

If YES:

Demand original electronic documentation: SWIFT MT535/MT536 messages (not PDFs), official custodian statements on letterhead with verifiable contact information, formal confirmation letters. If claimant cannot provide originals within 48 hours, treat as probable fraud and escalate. Screenshots are never acceptable primary evidence for transactions exceeding EUR 100,000.

Question 3: Does claimant claim direct CSD participation as private individual/small entity?

If YES:

This is impossible. CSD participation requires banking licenses, minimum capital of EUR 5-50 million, extensive operational infrastructure, and annual fees exceeding EUR 100,000. Private individuals and small private companies cannot meet these requirements. Immediate fraud escalation required.

Question 4: Are Bloomberg screenshots presented as ownership 'proof' or 'verification'?

If YES:

Bloomberg cannot verify custody holdings—this functionality does not exist. Any claim that Bloomberg confirms ownership demonstrates either fundamental ignorance or deliberate fraud. Demand actual custody documentation from CSDs or custodian banks. If Bloomberg screenshots are the only 'evidence' provided, treat as fraud attempt.

Question 5: Are 'blocked funds certificates' or similar documents presented without verifiable custodian confirmation?

If YES:

These documents are almost universally fabricated. CSDs do not issue 'blocked funds certificates' to beneficial owners. Demand independent verification: your institution must contact the stated custodian directly using contact information from the custodian's official website (never use contacts provided by claimant) to confirm the block's existence and authenticity.

Result Interpretation:

- **All five questions answered 'NO': Proceed to full verification protocol (Section 5)**
- **Any question answered 'YES': Immediate fraud escalation. Follow institutional fraud reporting procedures. Preserve all evidence. Do not continue engagement.**

Conclusion: From Knowledge to Action

CSD screenshot fraud represents the most persistent and financially material fraud vector targeting institutional finance operations. The technical knowledge presented in this document transforms institutional vulnerability into defensive strength—enabling personnel at every level to recognize fraudulent claims within seconds rather than discovering fraud only after weeks of wasted due diligence.

The fundamental reality bears repeating: Ultimate beneficial owners cannot and will not ever appear on CSD participant screens in omnibus account systems. This is not a configuration setting, not a privacy option, not an access control—it is a structural impossibility arising from the tiered architecture of international securities custody. Any screenshot showing individual names as CSD account holders is definitively, unequivocally fabricated.

The institutional imperative is clear: mandatory training for all client-facing personnel, rigorous enforcement of verification protocols, and zero tolerance for proceeding based on unverified claims. The cost of implementing comprehensive fraud detection capabilities is measured in tens of thousands of euros annually. The cost of failing to detect a single major fraud attempt ranges into millions of euros, compounded by reputational damage and regulatory consequences that can threaten institutional viability.

Every employee who reads this document gains the knowledge necessary to protect institutional assets and reputation. The responsibility now rests with leadership to ensure this knowledge translates into operational practice—through mandatory training programs, updated compliance procedures, and institutionalized verification requirements that make fraud detection automatic rather than dependent on individual expertise.

* * *

Document Version 2.1 | October 2025

*For additional resources, updated fraud intelligence, or training materials:
security.operations@infina.com*

© 2025 Institutional Finance Banking. All Rights Reserved.