

REVERSE LOGISTICS magazine®

Serving Manufacturers, Retailers, and Service Solutions Providers

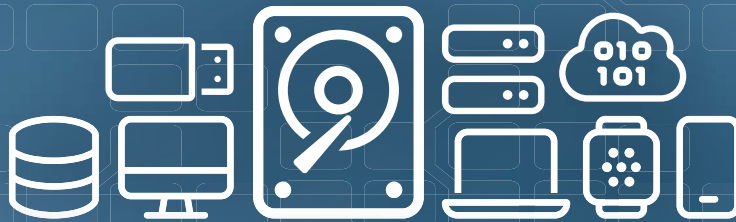


The 'Other' Customer –

Improving Customer Experience and Increasing
Loyalty for Buyers of Retail Returns



Erase data Permanently



Effortlessly protect your company's
privacy by securely erasing data
from all your devices.

Innovative Safeguards for Securing Transactions: How Mobile Retailers Tackle Counterfeit Mobile Device Returns

By Stephen Manning, CSO, FutureDial, Incorporated (RLA Bronze Member)

Fraud Fallout: The High Stakes Battle in Mobile Retail's Return Process

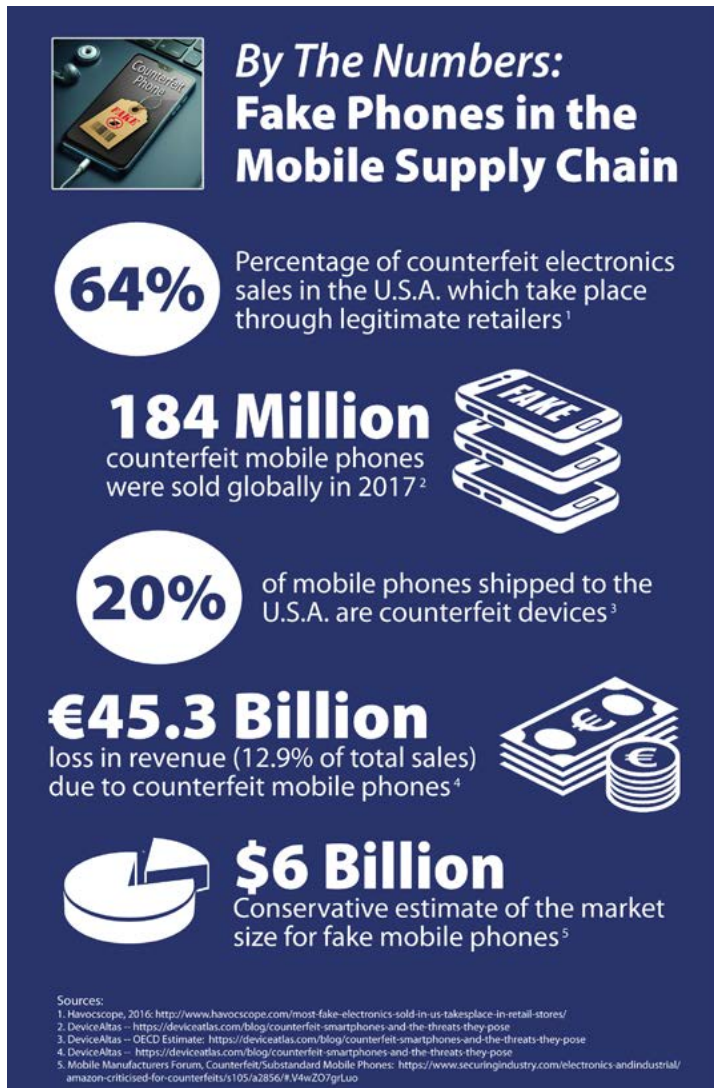
Mobile device retailers find themselves at the forefront of combating fraud and counterfeit returns, both at the point of collection as well as in online transactions. As the digital landscape evolves, so do the deceptive practices employed by unscrupulous individuals. To navigate this complex terrain, mobile retailers are harnessing advanced technologies, including A.I.-driven authentication and blockchain to secure transactions and protect against financial losses. Some ways in which fraud can occur include scenarios such as the following:

- Reselling of counterfeit phones
- Phones that are resold with defective parts
- Phones which were not properly authenticated prior to reselling
- Phones being traded-in or resold which were reported as lost or stolen

Safeguarding the Reverse Logistics Process Amidst Counterfeit Mobile Phone Proliferation

The massive impact of counterfeiting on the reverse logistics mobile supply chain is underscored by a comprehensive report from EUIPO-ITU. This global study estimates that counterfeit activities significantly affect smartphone sales, impacting a staggering 184 million units valued at 45.3 billion

EUR. This constitutes a substantial 12.9% of total sales, posing a formidable threat to both consumers and businesses operating within the mobile phone industry. Counterfeit phones, often priced

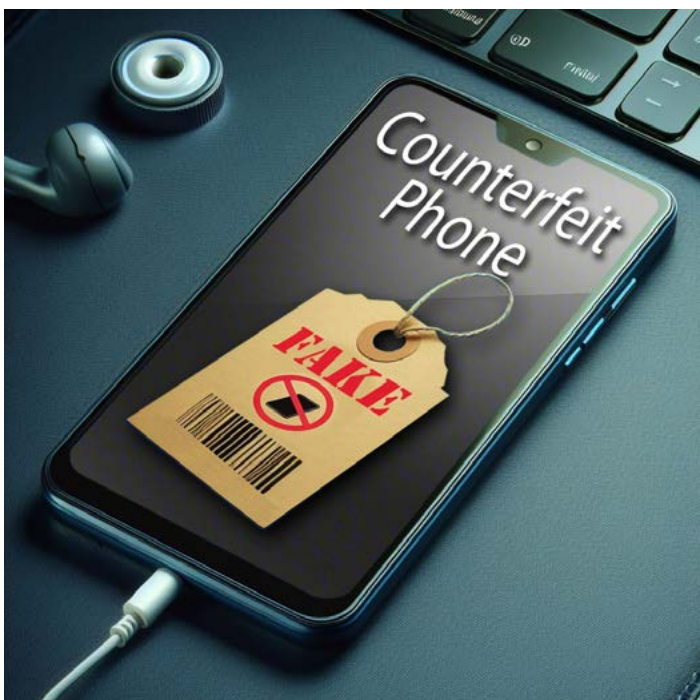


at a mere fraction of their authentic counterparts, are infiltrating the market through the expansive channels of widespread e-commerce platforms. This accessibility amplifies risk, as consumers may unwittingly purchase fake devices at one-tenth of the price, only realizing the deception when confronted with operational issues.

The pervasiveness of counterfeit phones further exacerbates the challenges faced by the reverse logistics mobile supply chain. According to OECD, the counterfeit phone industry accounted for approximately 20% of all mobile phones shipped internationally. The scale of this issue becomes even more alarming when considering the estimated loss in revenue, a staggering €45.3 billion annually, resulting from the sale of 184 million fake smartphones. Notably, prominent brands such as Samsung, iPhone, Xiaomi, OPPO, and Huawei find themselves among the most copied smartphone brands.

Understanding the Tactics: Return Fraud and Counterfeit Returns

Return of goods within the reverse logistics mobile supply chain is a focal point for combating fraud. Retailers face challenges as shoppers exploit gaps



in policies and return processes. Recognizing tactics related to return fraud and counterfeit returns is crucial for safeguarding against financial losses and maintaining operational integrity. Retailers must employ advanced technologies and stringent verification processes to prevent fraudulent returns.

“Fraud is prevented by establishing a strong traceable process on the front-end that leverages extensive data capture of the products prior to releasing to the Customer,” noted Jordan Sielaff, Co-Founder and CEO at Gierd, Inc., a company that specializes in helping businesses in the USA and EU to perform authentication of products across various sales channels. “Product Image, IMEI, shipment tracking, address verification and activating programs with the retailers to rely on the process/system and prevent fraudulent buyers from winning the war on theft,” he explained.



*Jordan Sielaff,
Co-Founder and CEO
of Gierd Inc.*

Mr. Sielaff emphasized that aside from counterfeiting, prevalent methods of online shopping theft encompass:

- False "Delivered Not Received (DNR)" claims, where customers falsely assert non-receipt, inflating costs.
- Illicit purchases using stolen credit cards.
- Address Fraud: during delivery, customers use non-inhabited or third-party business addresses to cross-dock products obtained through stolen credit cards.

To combat these issues, Mr. Sielaff suggested implementing reliable systems that foster trust throughout the sales process, thereby preventing fraudulent customers from successfully engaging in these types of theft activities.

Unveiling How Mobile Retailers Conquer Deceptive Tactics with Tech

Addressing fraud in mobile retail, especially in online trade-ins and transactions, has become increasingly challenging due to evolving deceptive tactics and system vulnerabilities. Online transactions offer fraudsters anonymity to exploit with false information and manipulated device conditions.

To combat these challenges, some retailers are proactively adopting advanced technologies:

(1) A.I.-Powered Verification:

Utilizing artificial intelligence to scrutinize device conditions and user behavior, identifying anomalies to differentiate between legitimate and fraudulent transactions.

(2) Blockchain Technology:

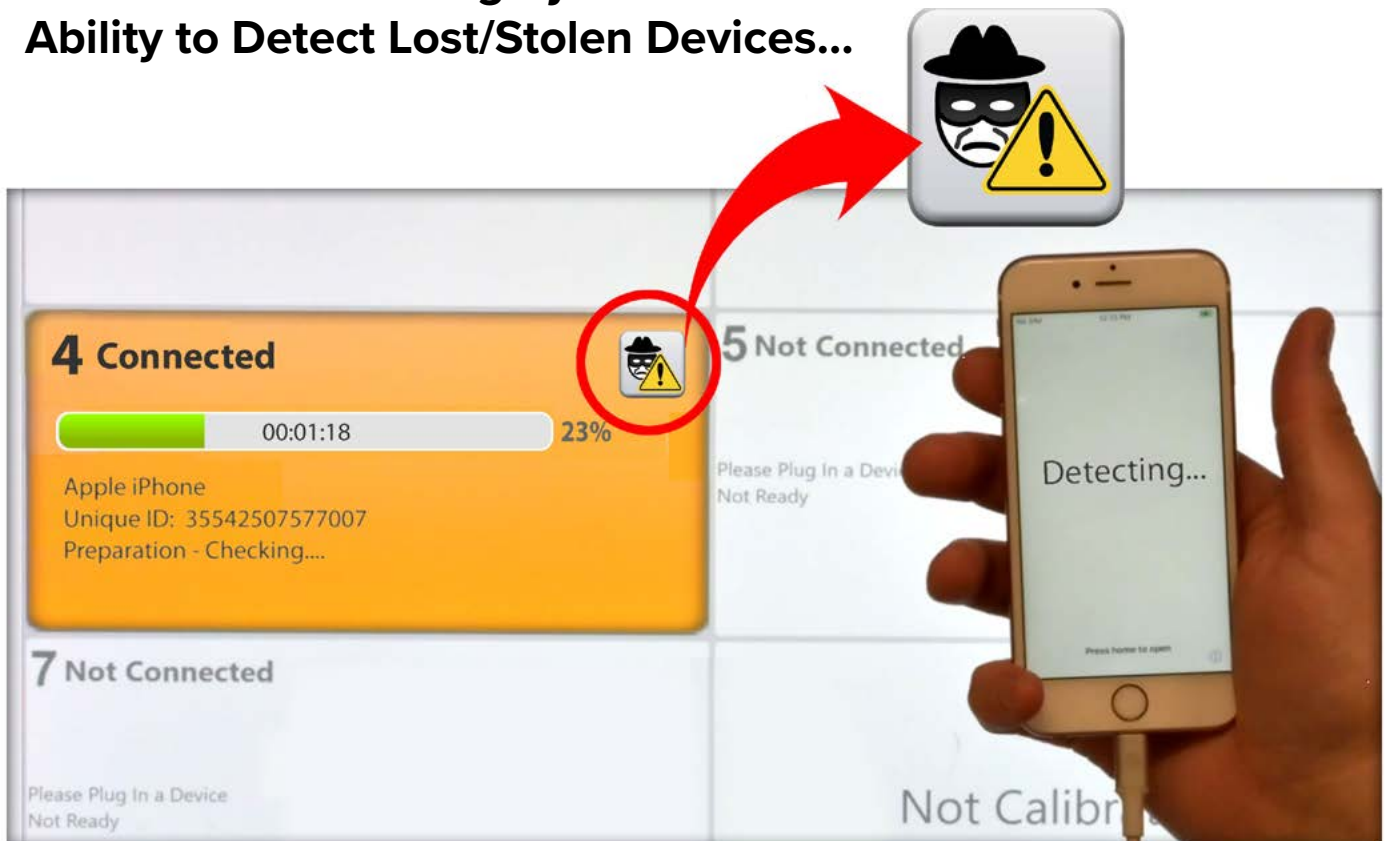
Offering a decentralized and distributed digital ledger system for transparent and secure transactions, mitigating risks linked to fraudulent returns.

The fusion of A.I.-driven authentication and blockchain strengthens transaction security and enables retailers to stay ahead of fraud.

Some leading companies providing authentication technologies to help combat fraud include:

- Prolog Mobile (<https://prologmobile.com/>) : Prolog Mobile pioneers mobile device analytics and transactions, offering comprehensive solutions in IMEI analytics, API services, and carrier compatibility, delivering value-based decisioning analytics for the global reverse supply chain.

Some Phone Processing Systems have the Ability to Detect Lost/Stolen Devices...



(Image Source: FutureDial Inc. Lean One-Touch™ Software)



transactions every day for law enforcement, wireless carriers, insurers, recyclers, retailers and consumers.

- Device Forensic (www.deviceforensic.com) : Technology developer for mobile device IMEI identification and verification, and accurately identifying device model specifications and potential issues for the reverse supply chain industry.

The Shared Responsibility in Fraud Prevention

Addressing the rampant fraud and counterfeit returns in the mobile phone retail sector necessitates a concerted effort fueled by proactive technology adoption. As the industry progresses, it becomes imperative for all stakeholders to unite in devising and executing comprehensive strategies to detect and deter fraudulent practices. Moreover, consumers play a vital role by staying vigilant, making educated buying decisions, and acknowledging the risks linked with counterfeit products. In today's technology-driven landscape, combatting fraud isn't merely a task for retailers; it's a collective responsibility essential for upholding the integrity of the mobile phone market.

- Recipero (<https://www.recipero.com/>) : A leader in crime and fraud intelligence solutions for the world's mobile device communities, with a suite of powerful data gathering and intelligence solutions, which together contribute to millions of global decision making processes and



Stephen Manning

Chief Strategy Officer, FutureDial, Inc.

Stephen Manning, the CSO at FutureDial, Inc., has over three decades of extensive expertise in Information Technology across various global domains, encompassing ecommerce, wireless technologies, outsourcing, reverse logistics, operations, sales, marketing, and finance. At FutureDial, Stephen spearheads the company's sales and business development endeavors, collaborating closely with prominent entities in the mobile device reverse logistics sector, such as tier-1 wireless carriers, third-party logistics providers (3PLs), mobile network operators (MNOs) and mobile virtual network operators (MVNOs), as well as mobile device trade-in and buyback operators, and phone resellers. Prior to his tenure at FutureDial, Stephen held pivotal leadership positions, including Chairman and CEO at Recellular Inc., President and CEO at CloudMSP, and Senior Vice President at Solectron Global Services, among others, showcasing his versatile leadership capabilities. His rich career trajectory also includes notable roles at Sequel Inc., AT&T, and other renowned organizations. Stephen holds a Bachelor of Science degree in Economics and Finance from the University of Nebraska and is a Certified Public Accountant (CPA), underscoring his strong academic foundation and professional acumen.