

Fraud as a Service: The Industrialization of Telegram-Enabled Scam Networks

Executive Summary

The conviction of Ramzan Abubakarov in early 2023 serves as a landmark case study in the evolution of cyber-enabled financial crime. It highlights a shift from isolated fraudulent acts to a sophisticated "Fraud as a Service" (FaaS) model. By leveraging the features of the Telegram messaging platform, criminal actors have built a scalable, digital supply chain that connects stolen data, ready-made phishing tools, and money-laundering networks. **Critical Takeaways:**

- **Industrialization:** Fraud is no longer the sole domain of technical experts; specialized suppliers now sell the components of an attack, lowering the barrier to entry for less-skilled offenders.
- **Telegram as a Marketplace:** Beyond private communication, Telegram functions as a marketing, distribution, and networking layer for criminal services.
- **Massive Scale:** The Abubakarov operation alone was linked to over £1.9 million in losses, the compromise of 30,000 personal identities, and a database of over one million mobile numbers.
- **The Criminal Value Chain:** Fraud, cybercrime, and money laundering have merged into a single process where various actors handle specific stages—from data theft to final fund conversion.
- **Defensive Integration:** Financial institutions must move beyond monitoring the "final transaction" and adopt a holistic control stack that integrates cyber intelligence, behavioral analytics, and recipient-side monitoring.

The Abubakarov Case: A Profile in Modern Fraud

In February 2023, Ramzan Abubakarov of Hendon, London, was sentenced to three years' imprisonment for ten offenses, including fraud by false representation and supplying articles for use in fraud. His operation provides a blueprint for how modern scam networks function.

Scale of Criminal Assets

Upon his arrest, investigators seized devices containing:

- **Compromised Data:** Financial and personal information of more than 30,000 individuals.
- **Targeting Databases:** More than one million UK and international mobile phone numbers.
- **Technical Tools:** Customized phishing kits specifically designed to target major financial institutions.
- **Total Victim Losses:** Attributed losses exceeded £1.9 million.

Telegram: The Engine of the Criminal Marketplace

While Telegram is a legitimate platform, its functionality makes it an ideal environment for "industrialized" fraud. It has facilitated a migration of criminal activity from the "dark web" to more accessible "clear web" platforms. | Feature | Criminal Application || ----- | ----- || **Public Channels** | Broadcasting stolen credentials and advertising services to thousands of users. || **Bots** | Automating interactions, distributing information, and managing customers. || **Usernames** | Enabling communication without exposing a telephone number, maintaining perceived anonymity. || **Public Links** | Directing potential buyers from social media platforms (Facebook, TikTok) to criminal storefronts. || **Client-to-Server Encryption** | Providing a layer of protection for communications and data transfers. |

The Abubakarov Telegram channel served multiple functions simultaneously: a **storefront** for illicit goods, a **customer support desk** for technical issues, and a **status platform** to build criminal reputation through screenshots of successful frauds.

The "Fraud as a Service" (FaaS) Supply Chain

The industrialization of fraud is driven by a specialized division of labor. One actor no longer needs to possess the skills for every stage of the crime.

1. Data Aggregation (iChop.it)

Abubakarov created **iChop.it**, a web service for buying and selling compromised data.

- **Identity Profiles:** Complete profiles (name, address, DOB, security data) allow for account takeover, impersonation calls, or fraudulent credit applications.
- **Data Re-use:** Information from one breach can be matched with data from another to increase the profile's value and credibility.

2. Phishing Kits as a Service

Instead of coding from scratch, criminals purchase ready-made packages that imitate legitimate organizations.

- **Technical Support:** Suppliers often provide updates when banks change their websites, troubleshoot installation, and offer real-time notification panels to capture authentication codes as victims enter them.
- **Case Example:** A 2025 case saw an offender sentenced to seven years for creating over 1,000 such kits, distributing them via Telegram with ongoing maintenance services.

3. Monetization and Social Engineering

Stolen data is used to make social engineering attacks more convincing. A caller who already knows a victim's bank, address, and recent account activity can easily manufacture trust to manipulate payments or reset passwords.

Exploiting Public Financial Systems

The Abubakarov case revealed how these networks exploit government-backed programs. Fraudsters use stolen or synthetic identities to submit high volumes of electronic applications for:

- **UK Bounce Back Loan Scheme**
- **False tax-refund claims** These programs are attractive because they prioritize rapid distribution and rely on electronic data, which can be easily faked using documents and instructions purchased from criminal marketplaces.

The Laundering Infrastructure

The financial harm of these platforms is realized only when proceeds are successfully laundered. This infrastructure typically involves:

- **Money Mule Networks:** Recruited individuals or compromised accounts used to receive and move funds.
- **Rapid Dispersal:** Funds are quickly moved through multiple accounts, withdrawn as cash, or converted into **cryptoassets** to obscure the trail.
- **Cryptoasset Payment:** Cryptocurrency is frequently used to pay for the illicit tools themselves (phishing kits, data sets) because it facilitates international movement outside traditional banking controls.

Strategic Recommendations for Financial Crime Leaders

To disrupt these networks, financial institutions and authorities must move from reactive to proactive, integrated defense strategies.

1. Integrated Control Stacks

Institutions should connect three traditionally separate areas:

- **Cyber Intelligence:** Monitoring for brand abuse and recovered phishing templates.
- **Fraud Monitoring:** Utilizing device and behavioral analytics to detect account access inconsistent with customer profiles (e.g., automated navigation or rapid credential testing).
- **AML Investigation:** Shifting focus to **recipient-side analysis** to identify mule clusters—accounts receiving payments from unrelated parties with rapid onward movement.

2. Proactive Platform Disruption

Disruption must target the business model, not just the content:

- **Platform Action:** Platforms must proactively detect channels sharing malicious domains or payment addresses linked to illicit markets.
- **Collaborative Intelligence:** Effective cases (like the Abubakarov investigation) rely on collaboration between banks, specialized units like the Cyber Defence Alliance, police, and tax authorities (HMRC).
- **Asset Recovery:** Treating investment fraud proceeds as money laundering enables the use of financial analysis to expose hidden account networks and freeze assets.

3. Strengthening Specific Controls

- **New-Beneficiary Risk:** Enhanced controls for payments to personal accounts presented as businesses.

- **Investment Fraud:** Identifying customers making repeated payments to unregulated recipients following social media contact, particularly in gold, forex, and oil "investments."
- **Credential Protection:** If a customer's credentials appear in a recovered criminal dataset, institutions must reset access and revoke active sessions immediately.