Due Diligence Report:

Hong Kong CipherChat Tech Company Limited and BonChat App

Subject: Potential Role as Infrastructure in Pig-Butchering / Ponzi Schemes, Including BG Wealth Sharing LTD and DSJ Exchange (DSJEX)

Compiled from Public Sources

This report synthesizes publicly available information on **Hong Kong CipherChat Tech Company Limited** (the developer) and its sole known product, the **BonChat** messaging app. It focuses on the company's structure, the app's features, and documented associations with organized cryptocurrency investment fraud networks (commonly known as "pig-butchering" or "copy-paste trading" Ponzi schemes). Particular attention is given to BG Wealth Sharing LTD / DSJ Exchange, as referenced in the query.

Important Note: This is **not** a formal investigation or legal opinion. It is based exclusively on open-source intelligence (company registries, app stores, regulatory alerts, victim reports, and investigative journalism). Government agencies should verify with primary sources (e.g., paid HK Companies Registry director filings, forensic app analysis, server logs, or international cooperation via MLAT/Interpol).

1. Executive Summary

- **Hong Kong CipherChat Tech Company Limited** is a recently incorporated private limited company (July 22, 2024) with a registered Hong Kong address and active status.
- Its only known product is **BonChat**, a cross-platform (iOS/Android) end-to-end encrypted (E2EE) messaging app emphasizing privacy, admin controls, and optional self-hosted/on-premise servers.
- **BonChat is an app** listed on official Apple and Google stores and functions as described. However, its design features have been identified as being **repeatedly exploited** by Chinese-run pig-butchering scam networks operating out of Southeast Asian compounds (notably Cambodia).
- The app has become a preferred communication tool for **BG Wealth Sharing LTD** and **DSJ Exchange (DSJEX)** operators. Scammers migrate victims from WhatsApp/Telegram to BonChat groups for "signal code" trading instructions, leveraging admin message-

deletion and blocking capabilities to erase evidence.

- Multiple international regulators have issued public warnings about BG Wealth / DSJEX as suspected Ponzi/pyramid schemes. Victim losses are documented in the hundreds of thousands per case.

- **Key red flags**: Extreme corporate opacity (no public directors/founders), rapid adoption by scam groups, and lack of independent security audits.

- **Recommendation**: Treat BonChat as high-risk infrastructure in ongoing cyber-fraud investigations. Pursue HK company filings for ultimate beneficial owners (UBOs), app-store metadata, and coordination with US/UK/Canadian/Australian/Asian authorities already alerting on BG Wealth / DSJEX.

2. Company Overview

- **Full Legal Name**: Hong Kong CipherChat Tech Company Limited (Chinese: **香港安雲科技有限公司**).

- **Incorporation Date**: July 22, 2024 (confirmed in official Hong Kong Companies Registry "List of Newly Incorporated Companies").

- **Business Registration Number (BRN)**: 76837457.

- **Registered Address**: Unit 1002, 10/F, Perfect Commercial Building, 20 Austin Avenue, Tsim Sha Tsui, Kowloon, Hong Kong (a shared/virtual office building commonly used by small entities).

- **Status**: Active / Live.

- **Transparency**: No publicly named directors, shareholders, or founders in free registry summaries. Paid services or official requests are required for full filings. No LinkedIn company page, press releases, funding announcements, or executive bios exist.

- **Contact Details (from app stores/website)**: support@ciphchat.com / admin@ciphchat.com; phone +852 6062 8732.

- **Scale**: Appears to be a micro-entity (likely <10 employees or outsourced development). No job postings, Glassdoor data, or evidence of other products/services.

3. Official Company / Product Website

- **Primary Domain: https://bonchat.app/**

- **Key Sections (as of April 2026):**
  - **Homepage:** Markets BonChat as "End-to-End Encrypted Chat Software with Private Deployment." Emphasizes secure messaging, file sharing, and on-premise options.
  - **About Us:** "CipherChat Tech, an innovative encrypted chat software company based in Hong Kong. We prioritize user security and privacy... Our expert team continuously enhances our software with the latest encryption technology." No named individuals or team details.
  - **Contact:** Confirms Hong Kong address and support email.
  - **Purchase / Buy:** Enterprise licensing and self-hosted deployment options (pricing starts in the thousands of USD).
  - **Other Pages:** Download links, FAQ, privacy policy (https://pub.bonchat.app/bonchat-privacy.html), version history.
- **Related Domains: bonchat.live (mirrors content), report.ciphchat.com (possibly for abuse reporting).**
- **Privacy Policy Highlights:** Company positions itself solely as the software provider; server operators (customers) handle data on self-hosted instances. No responsibility claimed for user content or group activity.

The website looks professionally presented but contains minimal substantive information beyond marketing claims — consistent with the overall low-transparency profile.

4. Product: BonChat App

- **Availability**: Official listings on Apple App Store (ID 6701998686) and Google Play under the exact company name.

- **Downloads/Ratings (as of April 2026)**: >1 million on Android; high ratings (~4.8 stars) but with increasing scam-related complaints.

- **Core Features (per developer description)**:
  - State-of-the-art end-to-end encryption for messages and files.
  - Cross-platform messaging, file sharing, group management.
  - **Advanced admin controls**: Group moderators can delete messages on **both sides** of a conversation and instantly block users.
  - Optional **private/on-premise/self-hosted server deployment** (enterprises or users can run their own servers for full data control).

    - Targeted at “privacy-conscious users, enterprises, and high-security scenarios.”

- **Developer Claims**: Emphasizes user privacy as a “fundamental right” with no backdoors mentioned. Company states it does not operate user groups or control content.

- **No Independent Audits**: No public third-party security review of the E2EE implementation or self-hosted server code was found.

5. Documented Misuse in Fraudulent Schemes

BonChat’s features (especially dual-side message deletion, blocking, encryption, and self-hosting) make it ideal for “dark room” operations where evidence disappears quickly.

- **Primary Scam Pattern (“Pig-Butchering” / “Click-a-Button” Ponzi)**:
    - Victims are groomed via WhatsApp/Telegram with romance or “wrong number” tactics.
    - They are migrated to **BonChat private groups** for the “investment phase.”
    - A “Professor” (or assistant) posts daily “signal codes.” Victims copy-paste these into the DSJ Exchange web platform to execute 60-second crypto futures trades.
    - Fake profits are displayed to build trust; small withdrawals may succeed initially.
    - Larger withdrawals are blocked with fees, “liquidity” issues, or account freezes.
    - Recruitment bonuses create a pyramid element.

- **Specific Link to BG Wealth Sharing LTD & DSJ Exchange (DSJEX)**:
    - Multiple regulators explicitly name these entities and note communication via **BonChat** (alongside WhatsApp/Telegram):
        - Alberta Securities Commission (ASC, Canada – Feb 2026).
        - Utah Division of Securities (Mar 2026).
        - Washington DFI (Apr 2026).
        - New Zealand FMA, UK FCA, Samoa CBS, Philippines, and others.
    - DSJEX websites (dsjex.net, dsj99.com, etc.) are described as unregistered fake trading platforms.
    - “Professor Stephen Beard” (likely fictitious) is frequently cited as the signal provider in BonChat groups.
    - Victim reports on Reddit (r/CryptoScams, r/Scams) detail family losses, evidence deletion in BonChat, and direct ties to BG Wealth / DSJ.

- **Broader Context – Southeast Asian Scam Compounds**:
    - These operations align with large-scale Chinese-organized cyber-fraud compounds in Cambodia (e.g., Sihanoukville), Laos, and Myanmar. US DOJ’s Scam Center Strike Force has targeted such networks for pig-butchering crypto scams involving human trafficking and forced labor.

- Encrypted apps like BonChat enable coordination and victim management with minimal traceability.

6. Regulatory & Victim Impact

- **Official Alerts**: At least 8 jurisdictions have warned the public about BG Wealth / DSJEX (listed above).
- **Victim Reports**: Widespread on Reddit and social media; individual losses documented in the $100K–$300K+ range. Families report grooming, pressure to recruit, and strained relationships.
- **App Store Complaints**: Direct reviews accuse BonChat of enabling scammers; developer responses deflect to "report to authorities."

7. Red Flags & Risk Assessment

- **High**: Corporate opacity + rapid incorporation in Hong Kong (common for Chinese scam-adjacent entities).
- **High**: Features explicitly useful for evidence destruction.
- **Medium-High**: No audits; self-hosted servers could be operated by bad actors.
- **Low**: No evidence the company itself steals funds or runs the scams—**it supplies the tool**.

8. Recommendations for further investigation

- **Immediate**: Request full HK Companies Registry filings (directors, shareholders, UBOs) and trademark records.
- **Forensic**: Analyze BonChat APK/IPA for server endpoints, self-hosting code, and logging. Coordinate with Apple/Google for developer metadata and takedown if warranted.
- **International Cooperation**: Share with ASC, FCA, FMA, US DOJ Scam Center Strike Force, and Cambodian/Chinese authorities.
- **Victim Support**: Cross-reference BonChat group IDs or "Professor" accounts with ongoing BG Wealth / DSJEX cases.

- **Monitoring**: Track enterprise/self-hosted deployments that may serve as private scam servers.

Conclusion:

BonChat functions as **enabling infrastructure** for sophisticated, multi-jurisdictional fraud networks centered on schemes like or adjacent to BG Wealth Sharing and DSJ Exchange. While the company appears registered, its product's popularity among operators linked to Cambodian scam compounds warrants prioritized scrutiny.

Sources:

Official HK registry documents, multiple regulatory investor alerts (ASC, Utah DFI, etc.), Reddit victim threads, BehindMLM investigative reports, US DOJ announcements, and app-store listings (full citations available upon request or via the referenced public URLs).
This report can be shared or expanded with additional primary data. Please provide any specific agency contact or further details (e.g., particular group IDs or victim statements) for targeted follow-up.