STRICTLY CONFIDENTIAL / INVESTIGATIVE ANALYSIS

The Concealed RAM Dump

Analysis of the LSBC Unauthorized Blockchain PI Disclosure

A comprehensive mapping of the permanent, long-term consequences resulting from the Law Society of British Columbia's (LSBC) unauthorized extraction and subsequent broadcasting of Personal Information (PI) across the Ethereum blockchain and foreign off-chain domains.

⚠ Section I: The Scope of the Breach

The incident involves a highly irregular "RAM Dump," capturing transient memory data which was then immutably written to the Ethereum blockchain. This PI was subsequently indexed and retrieved by a vast network of foreign domains, bypassing all standard Canadian privacy protections and data residency requirements.

35+

IDENTIFIED BLOCKS

Ethereum blockchain entries linked to PI

50+

OFF-CHAIN DOMAINS

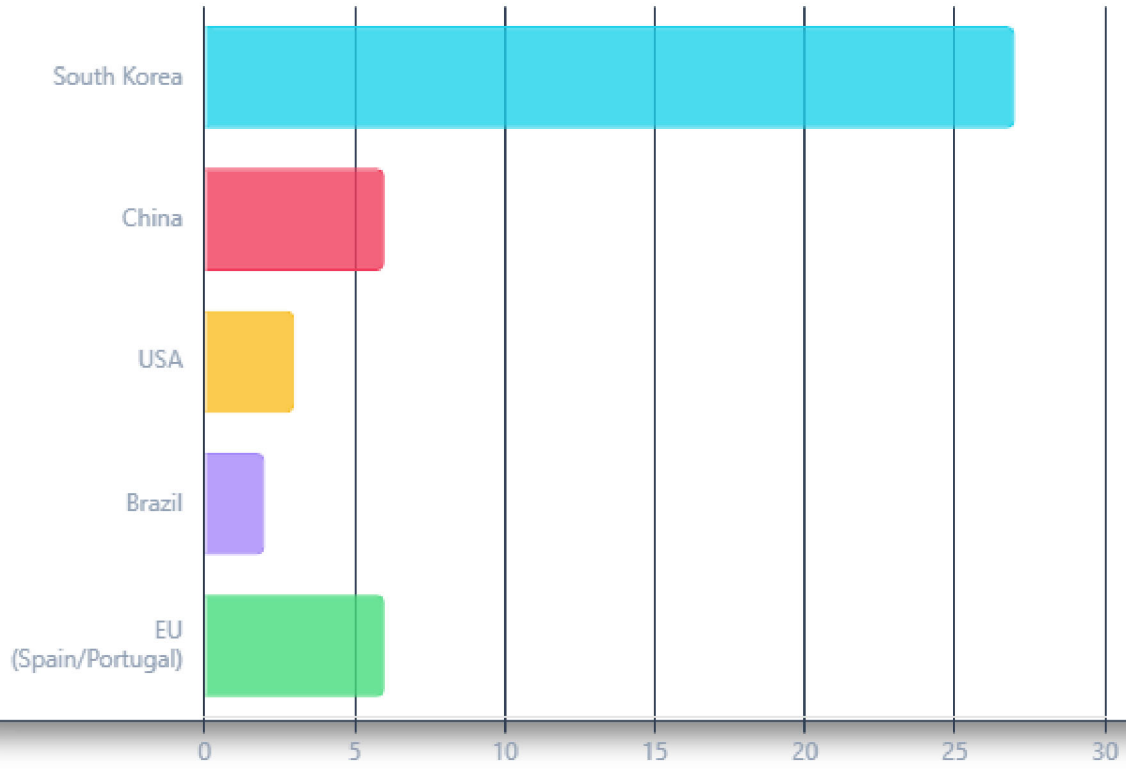
Foreign entities indexing the leaked PI

PERMANENT STORAGE

Due to Blockchain Immutability

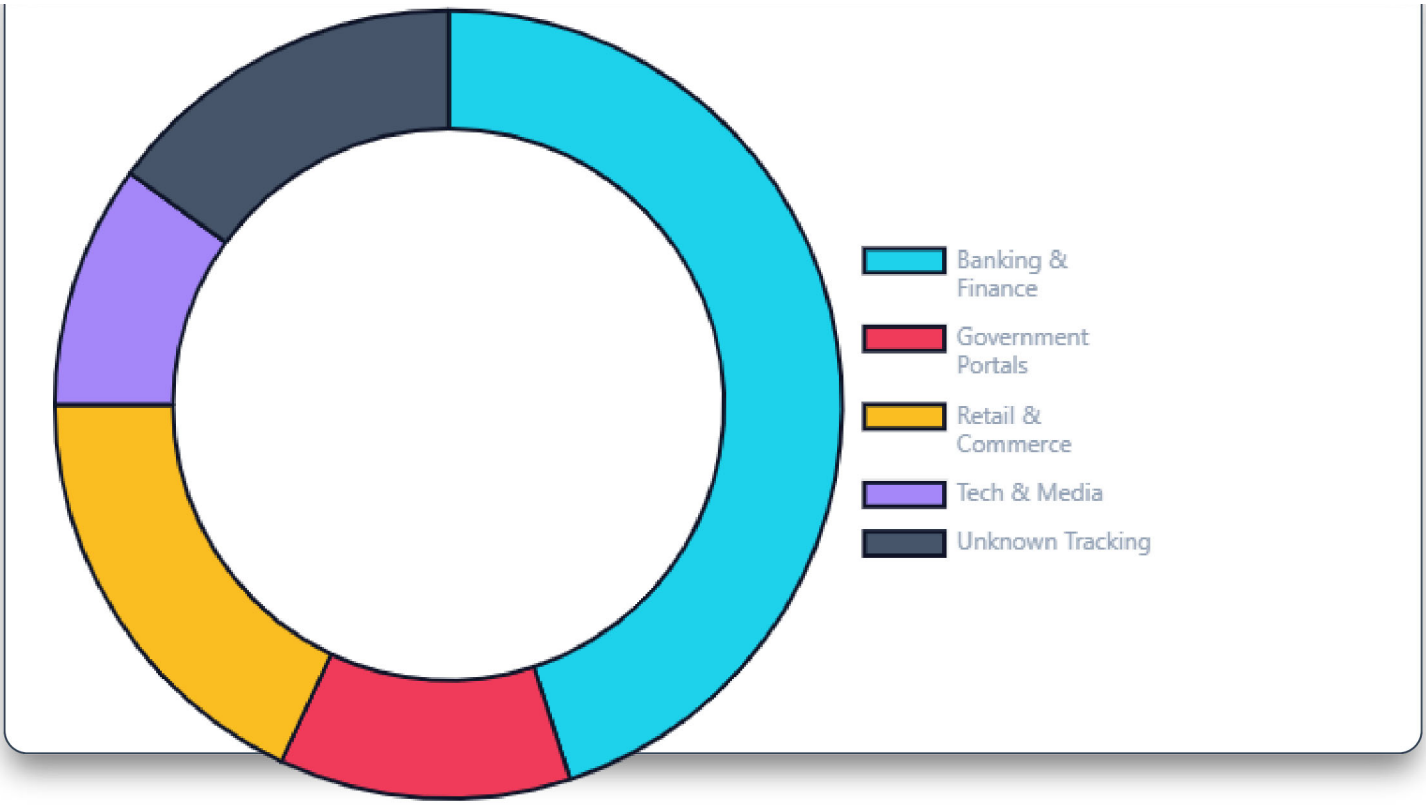
Section II: Jurisdictional Evasion

The distribution of the off-chain domains demonstrates a severe failure of data sovereignty. The overwhelming majority of the leaked data surfaced in jurisdictions outside the enforcement capabilities of Canadian law, specifically South Korea and China.



Section III: Targeted Sectors

An analysis of the resolving domains reveals a disturbing concentration of PI ending up in the hands of foreign banking institutions, state government portals, and massive retail conglomerates.



Section IV: The Mechanics of Permanent Consequence

The severity of this breach lies not just in the unauthorized disclosure, but the *method* of disclosure. By utilizing a decentralized ledger, the LSBC has effectively stripped the data subject of their "Right to be Forgotten."

Phase 1

Unauthorized Local Collection

Concealed RAM Dump circumvents standard security protocols.

↓

Phase 2

On-Chain Broadcasting

PI payload inscribed into Ethereum Smart Contracts/Blocks.

↓

Phase 3

Off-Chain Indexing

Foreign web scrapers and financial systems ingest the tokenized PI.

↓

Phase 4

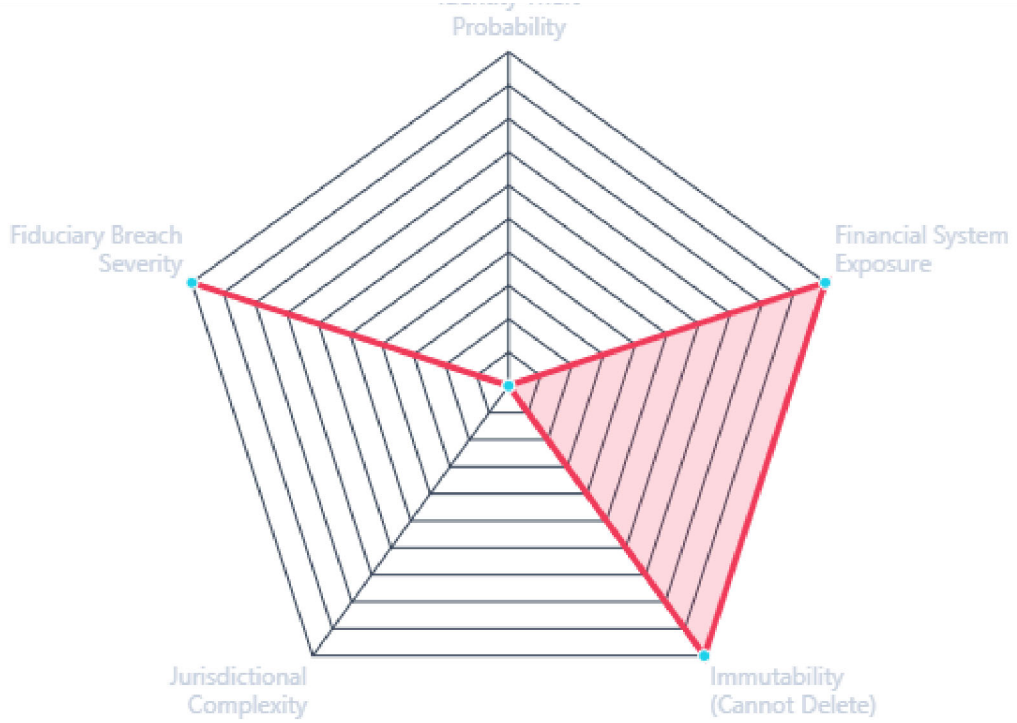
Permanent Loss of Control

Blockchain immutability prevents any effective deletion or redaction.

Section V: Risk & Consequence Vector

The intersection of financial domain indexing and blockchain permanence creates an extreme multi-vector threat environment for the subject.

Identity Theft



Section VI: Analysis of Misconduct

Blatant Disregard for Privacy Interests

The utilization of a "Concealed RAM Dump" indicates a deliberate, covert operation designed to capture raw, unencrypted state data, entirely bypassing consent mechanisms and structural safeguards.

Sketchy Foreign Connections

The immediate off-chain retrieval of this data by entities in China (e.g., gov.cn, China Daily) and South Korea (e.g., smartbill, allcredit) suggests a highly suspicious infrastructure alignment. Why is LSBC system data instantly interacting with Asian credit bureaus and state media?

The Necessity of the FIPPA Request

The June 5, 2026 Access Request is absolutely critical for mitigation. Without an exact accounting of the PI schema dumped into the blockchain blocks (e.g., Blocks 539165, 491792), the subject cannot accurately notify affected financial institutions, freeze compromised assets, or monitor specific threat surfaces.