UDC 004

FRAUD AND DATA BREACHES IN THE FINANCIAL SECTOR OF KAZAKHSTAN: STATISTICS, ANALYSIS, AND THREAT MODELING

Otegenov Z.B

Satbayev University

Introduction

The digital transformation of Kazakhstan's financial sector has significantly increased the adoption of online banking, mobile applications, and remote customer services. Over 85% of banking operations in the country are now performed online, creating both opportunities for accessibility and new vectors for cyber threats. According to national cybersecurity reports and law enforcement data, the number of incidents related to fraud and unauthorized access to personal data has grown exponentially in recent years [1] [3-4].

Modern cyber fraud campaigns increasingly combine technical exploits with social engineering techniques, such as phishing and impersonation of official banking channels. Attackers exploit data obtained from large-scale leaks to enhance the credibility of their scams. These developments underline the need for a holistic approach to financial cybersecurity—integrating technical, procedural, and educational measures—to mitigate both technological and human vulnerabilities.

Statistical Overview for 2023–2025

Between 2023 and 2025, Kazakhstan witnessed a dramatic escalation in cyber-enabled financial crimes.

According to Forbes Kazakhstan, in 2024 citizens transferred approximately 11.4 billion KZT to online fraudsters, which represents a 2.8-fold increase compared to 2023 [1]. Nearly the entire amount of losses—about 11 billion KZT—was sustained by individual users, indicating widespread vulnerability among retail clients.

The television channel 24.kz reported that more than 6,000 fraudulent loans were issued in 2024 under stolen identities [2]. The main cause was the weakness

of remote identification (KYC) procedures and insufficient verification in online credit systems.

In 2025, the Ministry of Internal Affairs of Kazakhstan registered over 14,000 cases of online fraud, reflecting a 22% year-on-year growth [3]. The cumulative financial damage amounted to several billion tenge. Furthermore, the Ministry of Digital Development confirmed one of the country's most significant data breaches, which exposed personal information of around 16 million citizens [5].

The correlation between data breaches and fraud intensity is evident: the wider the circulation of personal data, the higher the success rate of social engineering and identity-based attacks. Stolen databases containing IINs (personal identification numbers), phone numbers, and addresses have become a key enabler of phishing and remote loan fraud schemes.

Threat Model of Kazakhstan's Financial Sector

Building upon incident reports by KZ-CERT [4] and analytical insights from ENISA [6], a specialized threat model was developed to illustrate the relationships between threat actors, vulnerable assets, and mitigation controls. The model follows the logic of the STRIDE framework, adapted to the realities of Kazakhstan's financial ecosystem.

Within this context, the primary threat actors include organized criminal groups employing "Fraud-as-a-Service" models, individual cybercriminals specializing in phishing and social engineering, and, occasionally, insider threats. The main assets of interest comprise customer personal data, online banking credentials, authentication channels (notably SMS-OTP), and KYC/AML databases shared across financial entities and microfinance organizations.

Systemic vulnerabilities arise from reliance on single-factor authentication, weak oversight of third-party data processors, and limited digital literacy among users. Prominent threats include credential phishing, SIM-swap attacks, DDoS disruptions, and large-scale data exfiltration [6].

To address these challenges, the model proposes the implementation of multi-factor authentication (MFA) utilizing biometrics and hardware tokens, the

development of centralized anti-fraud platforms enabling interbank threat intelligence sharing, and the establishment of a national data breach registry to notify affected individuals. Furthermore, the model underscores the importance of continuous public awareness campaigns on cyber hygiene and social engineering prevention.

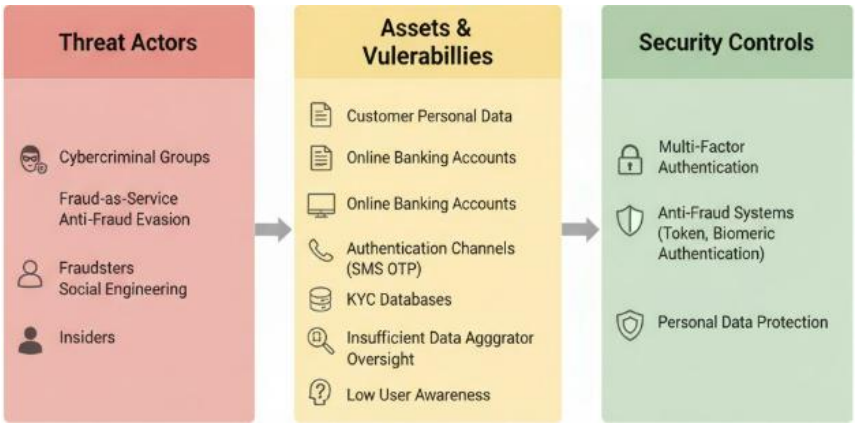

Figure 1 – Threat Model of the Banking Sector

The developed threat model in figure 1 reveals that phishing, fraudulent transfers, and unauthorized credit issuance constitute the most critical risks for Kazakhstan's financial sector. These threats demonstrate both high likelihood and severe impact, leading to significant monetary losses, reputational harm, and declining trust in banking institutions. Moderate risks are associated with data leakage through external vendors and DDoS attacks on financial APIs, while targeted Advanced Persistent Threats (APTs) remain infrequent but potentially devastating.

The root causes of most incidents are not purely technical. Organizational deficiencies, human error, and insufficient interinstitutional cooperation significantly increase overall exposure. The lack of a unified anti-fraud coordination framework among banks, telecom operators, and regulators hinders effective response and real-time threat mitigation. Establishing a centralized communication and monitoring platform would enhance collective defense and improve incident recovery efficiency.

Conclusion

The analysis confirms that cyber fraud in Kazakhstan has evolved into a systemic phenomenon. The combined losses from fraudulent transfers, identity-based credit issuance, and online scams have surpassed 11 billion KZT in 2024, with a steady upward trajectory in 2025. The most severe vulnerabilities stem from inadequate customer authentication mechanisms and the pervasive reuse of leaked personal data.

A transition toward proactive cybersecurity governance is imperative. This should include comprehensive MFA deployment, continuous behavioral fraud detection, creation of a national threat intelligence exchange, and robust legislation enforcing personal data protection. Strengthening public digital literacy remains equally critical: technological measures alone cannot ensure resilience without societal awareness and responsible user behavior.

Kazakhstan's financial institutions must thus adopt a predictive, intelligence-driven security model—one that combines data-driven analytics, regulatory coordination, and human-centered cybersecurity culture [6-7].

References:

1. Forbes Kazakhstan. Kazakhstanis transferred 11.4 billion KZT to fraudsters in 2024. – Available at: https://forbes.kz
2. 24.kz. Over 6,000 fraudulent loans issued using stolen identities in Kazakhstan. – Available at: https://24.kz
3. Ministry of Internal Affairs of the Republic of Kazakhstan. Report on cybercrime and online fraud in the Republic of Kazakhstan. – Astana, 2025.
4. KZ-CERT. Cybersecurity Incident Report, 1st Half of 2025. – Astana: KZ-CERT, 2025. – Available at: https://cert.gov.kz
5. Ministry of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan. Statement on the large-scale data breach of Kazakhstani citizens. – Astana, 2025.

6. European Union Agency for Cybersecurity (ENISA). Threat Landscape 2024. – Athens: ENISA, 2024. – Available at: https://www.enisa.europa.eu
7. ISO/IEC 27005:2018. Information security risk management. – Geneva: ISO, 2018. – 53 p.