PPIT Assignment 3

Zain Al Abidin 21L-6260, Murtaza Ahmed 21L-6234

1 Cyber-Crime Incident

1.1 Description of Cyber-Crime Incident

The FTX scam, led by Sam Bankman-Fried (SBF), represents one of the largest financial frauds in modern history. FTX was a cryptocurrency exchange that collapsed in November 2022, leading to losses exceeding $8 billion for investors. SBF was accused of misappropriating customer funds by transferring them to his trading firm, Alameda Research, to fund risky trades, political donations, and luxury real estate acquisitions.

The scam was executed by mixing customer deposits with Alameda's trading funds [1], violating the exchange's terms of service. This led to significant financial harm to investors and undermined trust in the cryptocurrency market. The collapse began with a leaked financial report in November 2022, revealing financial mismanagement and liquidity issues. He was convicted on all counts of fraud, conspiracy and money laundering.

1.2 Identification of Legal Framework

Sam Bankman-Fried was charged under the following legal frameworks :

- **Wire Fraud (18 U.S.C. § 1343)**: Alleging fraudulent schemes conducted over electronic communication.
- **Securities Fraud (Securities Act of 1933 and Securities Exchange Act of 1934)**: Relating to misrepresentation and manipulation of financial instruments.
- **Money Laundering (18 U.S.C. § 1956)**: Alleging illicit movement of funds to obscure their origins.
- **Commodities Fraud (Commodity Exchange Act)**: Covering fraudulent activities involving cryptocurrency.

These laws formed the foundation under which Bankman-Fried was prosecuted, resulting in a total of 7 charges filed by the U.S. Department of Justice (DOJ), the Securities and Exchange Commission (SEC), and the Commodity Futures Trading Commission (CFTC).

1.3 Analysis of Legal Response

He was sentenced to 18 years in prison and the court ordered him to pay the sum of 11.02 billion in forfeiture [2]. The legal response by U.S. authorities was not just considering the amount of money that was stolen. Bankman-Fried was arrested in December 2022 and extradited from the Bahamas to face charges. Investigations by the DOJ, SEC, and CFTC highlighted major systemic failures in operations and governance at FTX. However, there we challenges due to the complexity of cryptocurrency regulations and the absence of specific laws governing crypto exchanges. Some even argue that SBF was let off the hook because his parents were reputable people and had connections with strong people within the government

The effectiveness of the response was mixed. While the charges justified the misuse of customer funds, the lack of comprehensive cryptocurrency regulations exposed gaps in accountability. The case required the need for international cooperation since the funds and transactions spanned multiple jurisdictions.

1.4 Comparison with Local Incident

A similar incident that occurred in Pakistan was the Investors Club Scam in 2022, where a fraudulent investment scheme promised high returns via cryptocurrency. The Federal Investigation Agency (FIA) investigated the case under the Prevention of Electronic Crimes Act, 2016 (PECA) and sections of the Pakistan Penal Code (PPC).

Unlike the U.S., Pakistan's response was very limited due to practically no expertise in cryptocurrency and the absence of competent officials. The FIA faced challenges in tracing funds and prosecuting perpetrators due to jurisdictional limitations and lack of cooperation from international exchanges. This comparison highlights the need for stronger global partnerships and local expertise to combat such crimes effectively.

2 Privacy-Related Incident

2.1 Description of Privacy-Related Incident

The National Database and Registration Authority (NADRA) is responsible for maintaining the personal data of Pakistan's citizens, including sensitive information such as names, addresses, biometric details, and family structures. In recent years, there have been multiple reports of data breaches, with unauthorized individuals and entities gaining access to NADRA's sensitive database [4].

One notable incident occurred in 2021, when reports emerged of leaked data being used for unauthorized activities, including identity theft and illegal SIM card registration. The

breach highlighted vulnerabilities in NADRA's security infrastructure, raising concerns about the safety of citizens' personal information.

The consequences of these breaches were significant, as they compromised personal identities, leading to financial and reputational harm for individuals. Additionally, the leaked data was used in unauthorized activities, including criminal operations, further exacerbating the impact. These incidents also eroded public trust in government institutions responsible for safeguarding sensitive information, highlighting the need for stronger data protection measures.

2.2 Identification of Legal Framework

At the time of the incident, Pakistan relied on the following laws and frameworks:

- **Prevention of Electronic Crimes Act, 2016 (PECA 2016):** [3] This law criminalizes unauthorized access to and misuse of data. However, it lacks comprehensive provisions specific to large-scale privacy breaches.
- **Pakistan Penal Code (PPC):** General sections, such as those on fraud and forgery, were also applicable to misuse of leaked data.

Despite these legal provisions, Pakistan lacked a dedicated data protection law to address systemic privacy violations, leaving NADRA largely unaccountable for its data protection lapses.

2.3 Analysis of Legal Response

The legal response to the NADRA data leaks was inadequate in addressing the scale and complexity of the issue. While PECA 2016 criminalizes unauthorized access and provides penalties, it fails to mandate robust data protection protocols or impose liability on institutions like NADRA for negligence. Key shortcomings included the lack of enforcement mechanisms to ensure secure data handling by government agencies, the absence of legal obligations for notifying affected individuals in the event of a breach, and inadequate penalties to deter future violations. A comprehensive data protection law could have significantly improved the response to such incidents. For instance, establishing a dedicated Data Protection Authority could have enabled investigations and penalties for negligence. Additionally, mandatory breach notification protocols would have allowed citizens to take necessary precautions, while regular audits of data security measures could have mitigated risks effectively.

2.4 Comparison with International Frameworks

In comparison, countries like the European Union (EU) have robust privacy laws such as the General Data Protection Regulation (GDPR) [5]. Under GDPR, organizations are obligated to:

- Protect personal data with stringent security measures.
- Report breaches to both authorities and affected individuals within 72 hours.
- Face heavy fines for non-compliance, creating strong incentives for proactive data security.

Pakistan's reliance on outdated and reactive measures falls short of these international standards.

3 Conclusion

The FTX scam and the NADRA Data Leaks clearly highlight the evolving nature of cyber-crimes and privacy violations. Effective legal frameworks, international cooperation, and proactive governance are essential to addressing these challenges. Pakistan must enhance its legislative and technical capabilities to safeguard its digital ecosystem and protect citizens' rights.

References

[1] D. Yaffe-Bellany and E. Griffith, "How FTX's Sister Firm Brought the Crypto Exchange Down," *The New York Times*, Nov. 18, 2022. [Online]. Available: https://www.nytimes.com/2022/11/18/business/ftx-alameda-ties.html

[2] U.S. Department of Justice, "FTX Founder Sam Bankman-Fried Convicted of Fraud," Press Release, 2023. [Online]. Available: https://www.reuters.com/technology/sam-bankman-fried-be-sentenced-multi-billion-dollar-ftx-fraud-2024-03-28/

[3] Government of Pakistan, "Prevention of Electronic Crimes Act," 2016. [Online]. Available: https://pcsw.punjab.gov.pk/prevention-of-electronic-crimes-act-2016

[4] Dawn News, "NADRA Data Breaches Raise Privacy Concerns," 2024. [Online]. Available: https://www.dawn.com/news/1824026

[5] European Commission, "General Data Protection Regulation (GDPR)," 2018. [Online]. Available: https://gdpr-info.eu/