CYBERCRIME AND EFCC OVERSIGHT IN NIGERIA: LEGAL FRAMEWORK, ENFORCEMENT, AND BUSINESS IMPLICATIONS

Introduction

With the rapid digitalization of business and finance, cybercrime has emerged as one of Nigeria's most pressing legal and security challenges. Fraud, phishing, ransomware, identity theft, and hacking threaten individuals, companies, and critical infrastructure. The Economic and Financial Crimes Commission (EFCC) plays a central role in combating cybercrime, backed by Nigeria's legal framework. Understanding these obligations is crucial for businesses, fintechs, and online platforms to ensure compliance and protect stakeholders.

Legal Framework Governing Cybercrime

Key statutes include:

1. Cybercrimes (Prohibition, Prevention, Etc.) Act 2015
o Defines cybercrime offences, including:
- Identity theft
- Computer-related fraud
- Cyberstalking and harassment
- Financial scams

o Provides penalties ranging from fines to imprisonment.

2. Economic and Financial Crimes Commission (Establishment) Act 2004
o Empowers EFCC to investigate, prosecute, and prevent economic and financial crimes, including cyber-related offences.

3. Banks and Other Financial Institutions Act (BOFIA) 2020
o Mandates banks and financial institutions to report suspicious electronic transactions.

4. Data Protection Regulations – NDPR 2019
o Protects personal data; violations in the digital space can be linked to cybercrime.

5. Central Bank of Nigeria (CBN) Guidelines on Electronic Banking
o Requires banks and fintechs to implement robust cybersecurity measures.

EFCC Powers and Enforcement

The EFCC's mandate includes:
• Investigating cybercrime offences and digital financial fraud.
• Freezing or forfeiting assets obtained through cybercrime.
• Collaborating with INTERPOL, NITDA, CBN, and other agencies for cyber intelligence.
• Prosecution of individuals and corporate entities that facilitate, ignore, or fail to report cyber fraud.

Case Reference:

In EFCC v. Chukwudi Nwoke (2020), the court upheld EFCC's authority to prosecute large-scale online fraud operators, confirming the need for both individual and corporate accountability in digital transactions.

Cybercrime Risk for Businesses

Businesses face a dual risk:
1. Operational Risk – Direct financial loss due to hacking, phishing, and ransomware.
2. Regulatory Risk – Penalties for failing to report suspicious digital activities or protect customer data.

Non-compliance may lead to EFCC investigations, regulatory fines, and reputational damage.

PEARLTON ASSOCIATES
(LEGAL PRACTITIONERS)

Compliance Obligations for Businesses

1. Implement Cybersecurity Measures

• Firewalls, encryption, secure authentication, and intrusion detection systems.

• Cybersecurity audits and penetration testing.

2. Reporting and Cooperation

• Report cybercrime incidents to EFCC and other regulators promptly.

• Maintain logs of electronic transactions for investigative purposes.

3. Staff Training

• Educate employees on phishing, malware, social engineering, and proper reporting channels.

4. Data Protection and Privacy

• Ensure compliance with NDPR.

• Protect customer data to reduce exposure to cybercriminal exploitation.

Challenges and Areas for Improvement

• Low Cyber Awareness – Many businesses lack a basic understanding of cyber risks.

• Under-Resourced Enforcement – EFCC's digital forensic capabilities need scaling to match evolving threats.

• Cross-Border Crimes – Many cybercrime actors operate internationally, complicating prosecution.

• Insufficient Collaboration – Need for stronger partnerships between EFCC, NITDA, banks, and the private sector.

Recommendations

1. Adopt a Proactive Compliance Culture – Cybersecurity should be embedded in business strategy.
2. Invest in Technology and Forensics – Use AI, monitoring tools, and cybersecurity frameworks to detect and prevent fraud.
3. Strengthen Public-Private Partnerships – Share threat intelligence with EFCC and industry peers.
4. Regular Staff Training – Keep teams updated on evolving cyber threats.
5. Legal Readiness – Ensure contracts, policies, and terms of service address cyber liabilities.

Conclusion

Cybercrime in Nigeria is a growing threat with significant financial and reputational implications. EFCC's oversight, backed by the Cybercrimes Act and related legislation, provides the legal and enforcement framework to protect businesses and the economy. For businesses, compliance is not optional: implementing cybersecurity controls, reporting incidents, and training staff are essential to mitigate risk and ensure regulatory alignment. Proper vigilance, combined with proactive collaboration with EFCC and regulators, enables businesses to thrive safely in Nigeria's digital economy.