INCREASED CREDIT CARD CYBERCRIME - **A Call for Action**

(MENA FCCG)

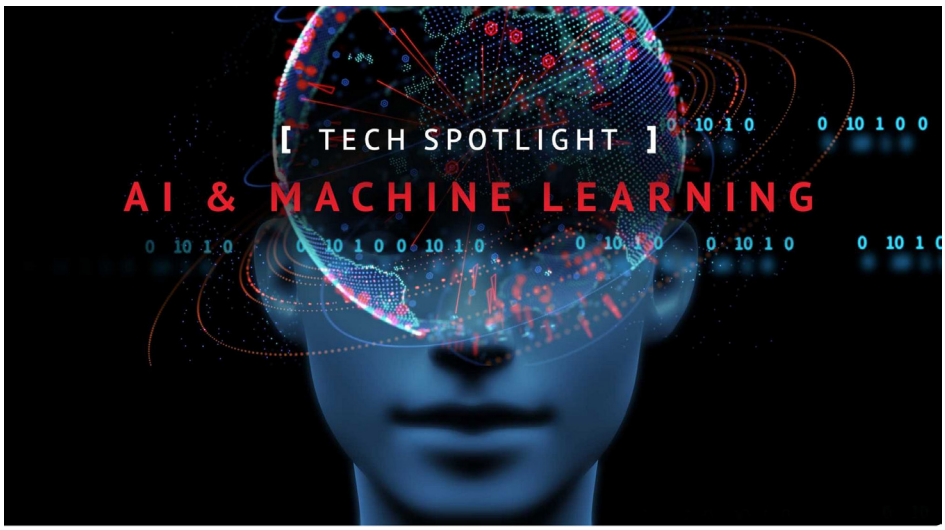
The MENA region is experiencing a significant increase in cybercrime associated with Card Non-Present transactions, which involve online purchases where the cardholder is not physically present. According to the INTERPOL Global Crime Trend Report of 2022, cybercrime rates in the MENA region are alarmingly high, with several countries ranking among the most targeted nations globally. The Dubai Police reported that four in 10 UAE consumers encountered online fraud attempts in 2020. Similarly, small businesses in Bahrain witnessed a staggering 348% surge in internet attacks between January and April 2022 compared to the previous year, as reported by Kaspersky.

With each iteration of PCI DSS standards, the underground criminal ecosystem continues to evolve, seeking to exploit any vulnerabilities that may arise. Cybercriminals have advanced beyond conventional techniques used in physical environments, such as skimming credit cards at Point of Sale (POS) terminals; instead, their focus has shifted to the realm of E-commerce, employing an array of sophisticated methods. This calls for heightened awareness and need for proactive measures to address the growing threats associated with increased credit card cybercrime.

As e-commerce businesses connect to a cloud provider for payment processing, security vulnerabilities such as insecure payment gateway integration, weak authentication mechanisms, outdated e-commerce platforms, malware and hacking, insider threats, vulnerabilities in third-party service providers, lack of encryption, and improper management of database encryption keys can potentially grant cybercriminals access to critical card data. Cybercriminals exploit these vulnerabilities, leaving real-world victims in their path. This can be equally detrimental to a bank's reputation, as most customers do not differentiate between the organization and other actors in the payment chain.

While MENA banks have continually scaled up prevention and containment measures including via frequent risk-sensitive penetration testing, certifications upgrade, & ensuring cardholders are knowledgeable of latest cybercrime tactics, two evolving areas demand increased knowledge and focus to effectively manage the heightened risks.

SECURING ARTIFICIAL INTELLIGENCE (AI) AND MACHINE LEARNING (ML) SYSTEMS



Cybercriminals generally exploit emerging technologies such as artificial intelligence (AI) and machine learning (ML) for password guessing attacks, circumventing CAPTCHA mechanisms designed to verify human users on websites, perpetrating human impersonation on social media platforms, and other vulnerabilities in susceptible hosts.

Recognizing the potential amplification of cybercriminal sophistication and reach enabled by AI/ML, it becomes imperative for banks to comprehend these technologies in order to protect their customers' sensitive information.

Machine learning models play a crucial role in recognizing malicious credit card transactions. The initial step involves gathering and organizing raw data to train the model in predicting the likelihood of fraudulent activities. This entails employing algorithms like logistic regression, random forests, support vector machines (SVMs), deep neural networks (including auto-encoders, long short-term memory (LSTM) networks, and convolutional neural networks (CNNs)). Furthermore, banks can leverage credit card profiling techniques and outlier detection methods to ascertain whether the cardholders or fraudsters are utilizing the credit cards. These approaches assist in identifying anomalous transactions, enabling the detection of credit card-related crimes such as money laundering and sanctions circumvention.

AI/ML enables card profiling that factors the cardholder's purchase history and other historical data, location, device ID, IP address, payment amount, transaction information, etc. The analytics-driven approach draws on both dynamic data, such as transaction flows, and static data, such as customer segments and geographical risk rankings. On the other hand, AI/ML also allows for data-driven analyses of merchants' role in the payment value chain, the types and segments of customers within their portfolios, their business models and product offerings, and their transaction flows in terms of volumes and types. The analysis sets the risk appetite and associated tolerance thresholds to monitor on an ongoing basis. In essence, AI/ML enables more nuanced cardholder and merchant segmentation models, based on real-time, up-to-date data to enable targeted detection and a clear ranking of customers and transactions.

Additional security considerations follow:

- Data Sources: In addition to purchase history and transaction information, other potential data sources for card profiling could include customer demographics, social media activity, and external data feeds such as fraud intelligence databases.

- Feature Engineering: AI/ML models for card profiling often require careful feature engineering, which involves selecting and transforming relevant attributes to maximize their predictive power. This step is essential for building accurate and effective models.

 Anomaly Detection: Highlight the importance of utilizing AI/ML techniques for detecting anomalies in cardholder behavior or merchant transactions. This involves identifying patterns or behaviors that deviate significantly from normal or expected patterns, enabling the detection of potential fraudulent activities.

 Real-time Monitoring: Emphasize the ability of AI/ML to enable real-time monitoring and analysis of cardholder and merchant data. This allows for immediate detection of suspicious transactions or activities, facilitating prompt intervention and mitigation of risks.

 Adaptive Models: Ensure that AI/ML models used in card profiling are adaptive, meaning they can continuously learn and update their profiles based on new data and evolving patterns, enhancing their accuracy and effectiveness over time.

THE EVOLUTION OF CYBERCRIME AS A SERVICE (CAAS)

CaaS is an organized crime model, wherein "enablers" within the cybercriminal ecosystem sell their tools, expertise, and services to other cybercriminals. The structure of CaaS allows hackers to forego the need for extensive coding skills or the development of their own malicious software, instead becoming customers of more experienced cybercriminals who offer CaaS services. A CaaS operation exhibits business-like organization, involving engineers, leaders, and developers responsible for constructing and offering the services and tools. In some cases, CaaS providers even offer technical support representatives to assist buyers in understanding the intricacies of their products. Notably, CaaS encompasses various subcategories, such as Ransomware-as-a-Service (RaaS), Phishing-as-a-Service (PhaaS), and Malware-as-a-Service (MaaS), among others.

Given the lucrative nature of cybercrime, CaaS is becoming embedded into the underground economy and with a rising number of threat actors that offer CaaS services; the market becomes more competitive, resulting in lower prices and a wider range of diversified criminal services. Effectively managing associated risks requires banks to connect the dots and comprehend the critical junctions formed by online interactions among various actors in the cyber ecosystem. This task can be complex and daunting but is crucial for safeguarding against evolving threats.

A CALL FOR ACTION

Addressing the true human, societal, and economic impact of financial crime is a never-ending challenge that requires increased competencies to combat financial crime, as well as cross-border collective action from policy makers, governments, law enforcement, regulators, and financial institutions guided by their moral compass to make a difference in protecting their communities and economies.

Success requires a new paradigm, one that relies on openness between gatekeepers and organizations to better connect the dots, understand the cybersecurity ecosystem, and share perspectives and experiences including in the arena of AI/ML.

Increased public private collaboration as supported by the MENA Financial Crime Compliance Group (MENA FCCG), a group of 13 leading banks from the MENA region, as well as the Global Coalition to Fight Financial Crime (GCFFC), who are committed to make a collective impact in the fight against financial crime via capacity building and public private sector dialogue. Separately, MENA FCCG recently established a Sub-Committee on AI, consisting of Tech Leads (data scientists) from member banks to discuss latest technology initiatives and applications (AI, Advanced Analytics, ML, Robotic Process Automation (RPA), etc.) for combating financial crime including cybercrime. Via its AI arm, the Group is planning to issue a value-added white paper on the maturity of AI across MENA banks shedding light on AI/ML initiatives worth experimenting.

"WORKING TOGETHER, WE CAN MAKE A DIFFERENCE."

ABOUT THE AUTHORS

MICHAEL MATOSSIAN, EVP AND CHIEF COMPLIANCE OFFICER joined Arab Bank plc in November 2005 as EVP and Global Head of Group Regulatory Compliance. Mr. Matossian has more than 35 years of experience in Regulatory Risk Management, Anti-Money Laundering, and Corporate Governance. Mr. Matossian participates on several national and international task forces addressing anti-money laundering, privacy, and compliance matters and is the Founding Member and Deputy Chair of the MENA Financial Crime Compliance Group and Vice Chair of the Global Coalition to Fight Financial Crime - MENA Chapter.

ASHRAF SAMHOURI, HEAD OF LINE OF BUSINESS REGULATORY COMPLIANCE at Arab Bank is a Certified Anti-Money Laundering Specialist. Mr. Samhouri has more than 20 years of experience in Internal Audit, Regulatory Compliance Risk Management, and Combatting Financial Crime. He holds Master of Business Administration (MBA) from University of Jordan. Mr. Samhouri regularly participates as a trainer in various compliance related topics including Digital Transformation & Innovation, Treating Customers Fairly, Enhancing the Role of the First Line of Defense, and Increased Regulatory Expectations for Financial Institutions.

ABOUT MENA FCCG:

The MENA Financial Crime Compliance Group (MENA FCCG) is a voluntary body that seeks to bring collective action in the fight against money laundering and terrorist finance in the region. The Group comprises 13 banks representing eight MENA countries, including Bahrain, Egypt, Jordan, Kuwait, Lebanon, Oman, Qatar, and the UAE. The Group is presided over by Dr. Wissam H. Fattouh, Secretary General for the Union of Arab Banks while Michael Matossian is the current Deputy Chair.

Member Banks:

Bank Audi · بنك أبوظبي التجاري ADCB · alBaraka · البنك العربي ARAB BANK · BankABC · بنك مسقط BankMuscat · بنك مصر Banque Misr · بنك بوبيان Boubyan Bank · Emirates NBD · المشرق mashreq · البنك الأهلي المصري National Bank of Egypt · الوطني NBK · QNB

The Group also seeks to enhance dialogue among public and private sector actors as the best medium for a more targeted and intelligent approach for responding to the changing face of financial crime. In November 2021, the Group officially launched a Europe Chapter at an inaugural meeting in London. The chapter aims to extend MENA FCCG's objectives to Europe by bringing together compliance professionals of Arab banks operating in Europe to enhance financial crime literacy and support implementation of best practices. The Arab Bankers Association acts as the strategic partner and the Chapter has entered a strategic alliance with Themis Services, a specialist financial crime consultancy.

MENA FCCG Strategic Partners and Alliances

Strategic Partners

Union of Arab Banks · REFINITIV An LSEG Business

EU Chapter Strategic Partners

Arab Bankers Association جمعية المصرفيين العرب · THEMIS

Strategic Alliances

UNSC United Nations Security Council · the Wolfsberg Group · Global Coalition to Fight Financial Crime · ACAMS · K2Integrity