E-PAYMENT SYSTEM FRAUD AND COUNTERMEASURES

MR. GEORGE NKRUMAH

Outline of Presentation

- Overview of the Payment Ecosystem in Historical Perspective
- Situational Analysis & Current Developments
- ML/TF Risk associated with E-Payment Systems (Mobile Money, E-Banking, Prepaid Cards, ATMs, etc)
- Breakout Session
- Significant issues/gaps in addressing ML/TF Risks
- Institutional Best Practices to prevent AML Risks in the Payment Ecosystem.
- Case studies/Discussions

Overview of the Payment Ecosystem in Historical Perspective

BACKGROUND

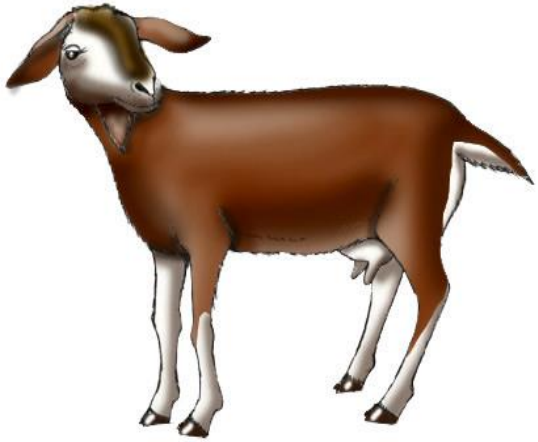
- Buying things and paying for them is something that is part of our everyday lives nowadays. However, the payment infrastructure dates back to ancient times when **barter** was the mode of payment.

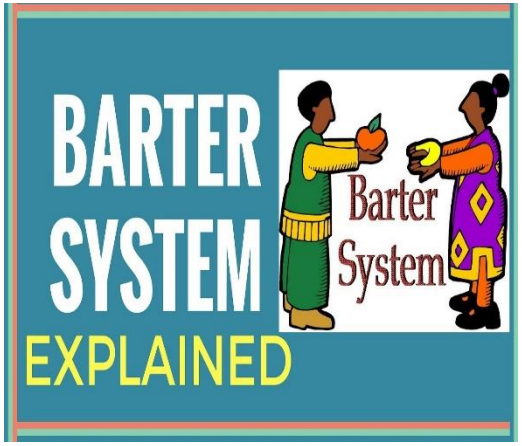
- An **example of barter** is when the people within a community exchange goods and services so that money need not be used. An **example of barter** is bread provided in exchange for butter.

- Consequently, the mode of payments has evolved from ***barter*** to ***gold backed money***, the use of ***coins and bank notes (fiat currency)***, ***negotiable instruments (personal cheques, travelers cheques, promissory notes, certificates of deposits and money orders)***, ***payment cards***, ***electronic money (E-Money)*** **and** ***Crypto currency*****.**

Overview of the Payment Ecosystem in Historical Perspective

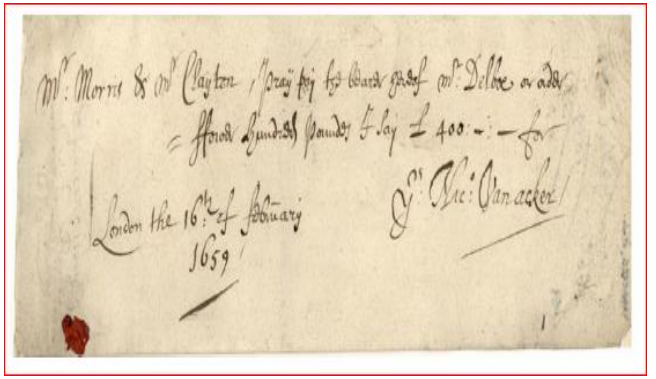
- **In the Beginning……..**
- *Large Purchases* *Small Purchases*





Overview of the Payment Ecosystem in Historical Perspective

Cheque invented: Persia, 550–330 BC.
Achaemenid Empire
India, Rome, Knights Templar used cheques



THE PAYMENT LANDSCAPE TODAY

- Online payment services (PayPal, WorldPay…)
- Electronic bill payments (Internet banking et sim.)

- Wire transfer (local or international)
- Direct credit, initiated by payer: ACH in US, Ghana and Europe
- Direct debit, initiated by payee

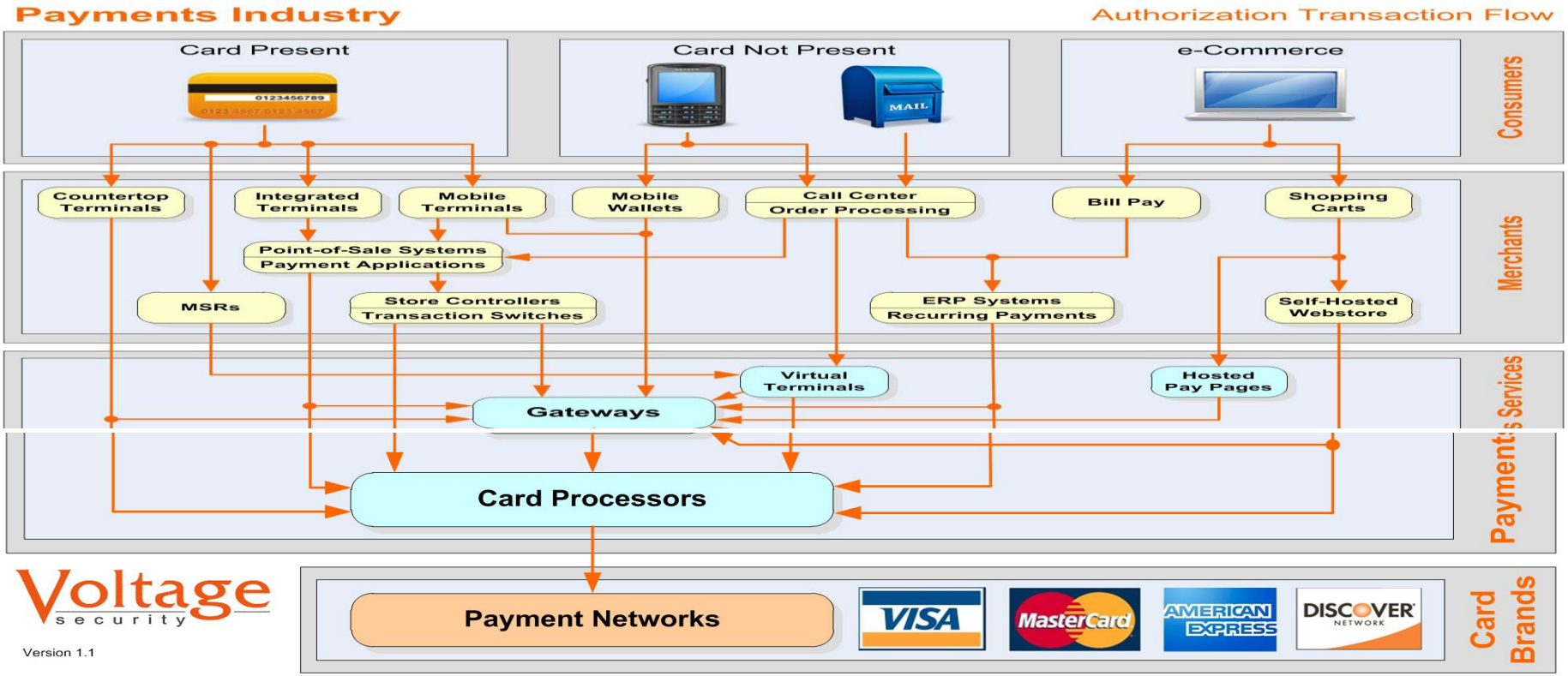
- Debit cards
- Credit card

PayPal

WorldPay

Situational Analysis & Current Developments

THE PAYMENT LANDSCAPE TODAY



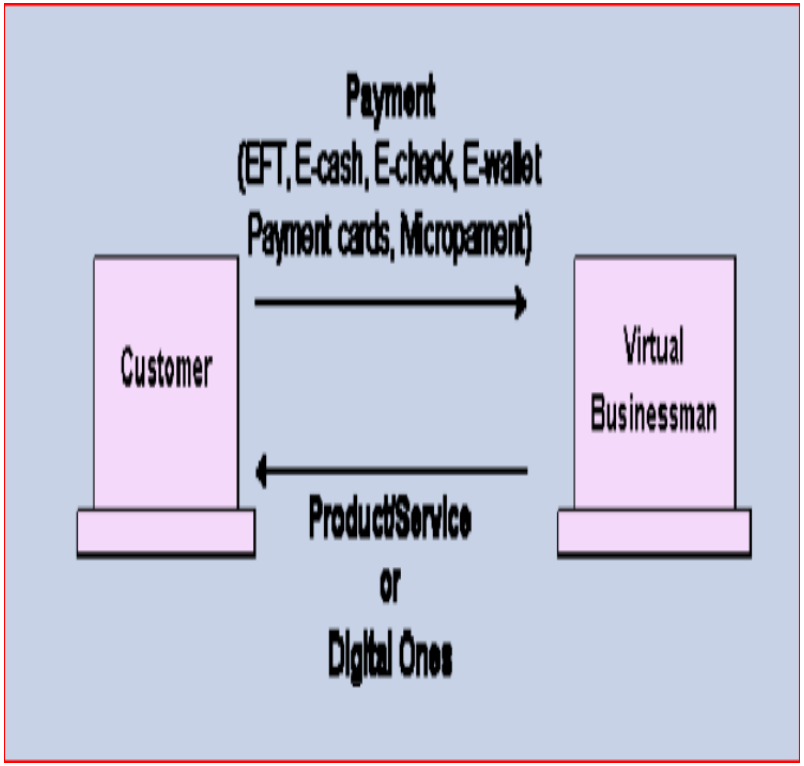
Situational Analysis & Current Developments

WHAT IS E-PAYMENT

- An e-payment system(EPS) is a way of making transactions or paying for goods and services through an electronic medium, without the use of cheques or cash. It's also called an electronic payment system or online payment system.

- EPS enable a customer to pay for the goods and services online by using integrated hardware and software system.

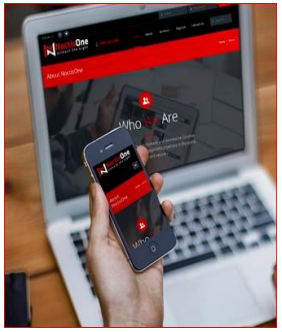
- Benefits of EPS are to increase efficiency, improve security, and enhance customer convenience and ease of use.

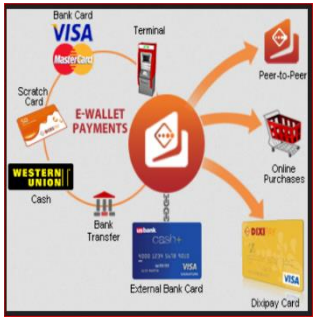


Situational Analysis & Current Developments

FORMS OF E-PAYMENT SYSTEM

- **Credit cards** to pay for products/services purchased online:
- **Electronic funds transfer (EFT):** EFT involves electronic transfer of money by financial institutions.
- **Payment cards/Credit cards/smart cards :** They contain stored financial value that can be transferred from the customer's computer to the businessman's computer.
- **Electronic money (e-money/e-cash):** This is standard money converted into an electronic format to pay for online purchases.
- **Online payment**: This can be used for monthly payment for Internet, phone bills, etc.
- **Electronic wallets (e-wallets) :** They are similar to smart cards as they include stored financial value for online payments.
- **Electronic gifts :** They are one way of sending electronic currency or gift certificates from one individual to another. The receiver can spend these gifts in their favorite online stores provided they accept this type of currency.





Situational Analysis & Current Developments

MARKET PLAYERS IN THE E-PAYMENT ECOYSYSTEM

DRIVERS OF E-PAYMENT ECOSYSTEM

- Changing consumer behaviour and expectations;
- E-commerce developments (emergence of (social) platform commerce and subscription commerce);
- Technology driven innovation;
- Regulatory reforms and frameworks to clarify aspects in the e-commerce and online payment ecosystem and financial inclusion.

BREAKOUT QUESTIONS

- What has been the impact of COVID-19 Pandemic on E-Payment Channels in your jurisdiction?
- How are Fintech and E-Payment Channels supervised in your countries?
- There is a general observation of an upsurge of E-Payment crimes. Give a situational analysis and typologies in your countries.
- What are the most common E-Payment Channels in your jurisdiction and what has been the motivation for these channels?

ML/TF Risk associated with E-Payment Systems

CUSTOMER RISK FACTORS

- Inability to transact due to network down time
- Complex and confusing user interfaces
- Non transparent fees and other terms
- Fraud that targets customers and
  by employees, fraudsters and agents
- Inadequate data privacy and protection

ML/TF Risk associated with E-Payment Systems Fraud Implications

ML/TF Risk associated with E-Payment Systems (Mobile Money, E-Banking, Prepaid Cards, ATMs, etc)

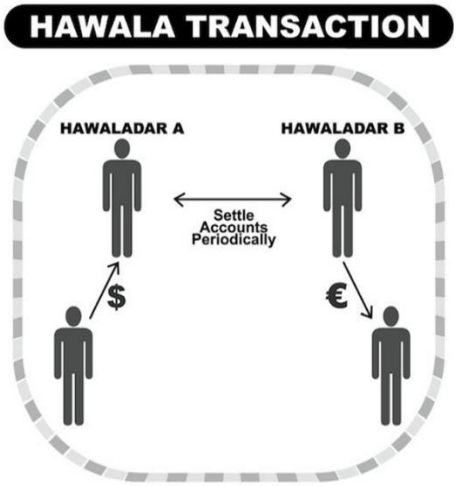
Transfers: Money wire transfers can be characterized as the easiest transfer method within the money laundering activities. The main abuses are as follow:

- The use of falsified or false **identities**
- Structured payment also called **Smurfing**
- A smurf is a colloquial term for a money launderer, or one who seeks to evade scrutiny from government agencies by breaking up a transaction involving a large amount of money into smaller transactions below the reporting threshold.
- Transfers through banks in **offshore** countries with customer identities protected from jurisdiction.

ML/TF Risk associated with E-Payment Systems

- Transfers as a result of criminal actions eg **hacking**
- Informal money transfer systems such as **Hawala**

- A traditional system of transferring money used in Arab countries and South Asia, whereby the money is paid to an agent who then instructs an associate in the relevant country or area to pay the final recipient.



- **Sakawa** is a Ghanaian term for illegal practices which combine modern Internet-based fraud with African traditionalist rituals. It involves on-line dating which involves promise of marriage etc.

ML/TF Risk associated with E-Payment Systems

Payment Interception

❑Payment interception, or also known as "man in the middle fraud," is when malicious people take over a payment process. Fraud is moving away from credit cards and into e-wallets and social media-based transactions. With payments now possible via Facebook messenger, fraudsters are taking over transactions by intercepting transactions in the middle of the sales process.

ML/TF Risk associated with E-Payment Systems

ML/TF Risk associated with E-Payment Systems (Mobile Money, E-Banking, Prepaid Cards, ATMs, etc)

- **Absence of credit risk**
  Funds for use with EPSs are generally prepaid. The absence of credit risk means that service providers may have fewer incentives to obtain full and accurate information about the customer and the nature of the business relationship.

- **Speed of transactions**
  NPM transactions can be carried out and funds withdrawn or converted much quicker than through more traditional channels. This can complicate monitoring and potentially frustrate efforts to freeze the funds.

- **Non-face to face business relationship**
  Many (but not all) EPS providers' business model relies on non-face to face business relationships and transactions, which increase impersonation fraud risk and the chance that customers may not be who they say they are.

ML/TF Risk associated with E-Payment Systems

- **Wire transfers** can be characterized as the easiest transfer method within the money laundering activities. Often the sender and the receiver of the transferred money may be the same person who tries to conceal the origin of money by several money movements (transfers).

- **Prepaid/Smart cards -**In this example funds received from the activities of drug trafficking and placed on a smart card. Their small size, these cards can be easily and safely hidden, and ultimately to be cashed out through re-Deposit, but in a foreign country.

- The second route is beyond the reach of the powers of law enforcement as the transfer of funds on the card through an e-payment medium such as mobile money makes it indistinguishable from funds derived from legitimate sources once it enters the e-payment system.

- For terrorist financing the account-unlinked products (with just e-purse functionality) are more attractive; they allow loading of currencies, e.g., in exchange of cash.

ML/TF Risk associated with E-Payment Systems

- **Remittances through system based on the Internet -**In this example with low nominal card value is passed to personal computers, which transmit this value over the Internet, using increasingly available anonymous services to hide the entry points for illicit funds. The recipient of the funds has the ability to unite the payments and re-integration back into the payment system.

- **Electronic money-**The latest example of the illegal use of electronic payments carried out under the banner of mercy, which serves only as a cover for receiving transfers in the form of donations. The funds, originally created as a charity, and honestly carrying out his mission, however, could act as one link of the chain of laundering criminal funds using electronic payment systems.

GAPS

- The FATF Recommendations require all entities or persons conducting certain activities to be subject to AML/CTF obligations and oversight. These include entities or persons transferring money or value, or issuing and managing means of payment. In Ghana BOG regulates financial Institutions and National Communication Authority (NCA) regulates the mobile companies. Lack of coordination.
- To bridge this gap, a Payment services act (Act 987) as passed to make BOG the supervisor of all these intermediaries. These includes
  - Banks
  - Special Deposit taking Institutions (SDIs)
  - A Payment service provider
  - Affiliates and agents of banks and SDIs
- Mobile payment service providers often use agents for the distribution of their services, opening new customer accounts, as well as receiving and paying out cash from or to customers. Such agents typically are numerous and are themselves not subject toimmediate regulation.
- Mobile payment services allow third-party funding which can be exploited by criminals.

Significant issues/gaps in addressing ML/TF Risks

Like any financial product, there are inherent risk and ML/TF is one of the risk that has to be identified and mitigated.

The following mitigants can help reduce the use of EPS by money launderers;

- ***Value limits***
  Applying a risk-based approach on value limits of the various forms of e-payment can discourage the use of the e-payment system by money launderers.

- ***Transaction Monitoring and Fraud Detection Tools***
  EPS are based on computer technology and therefore provide good prerequisites for effective monitoring and reporting procedures. Transactions carried out through the system always leave electronic footprints which can be monitored and analyzed
  This means that providers can block accounts where they detect abnormal transaction patterns or otherwise become suspicious that their product might be abused for ML/TF purposes.

.

Significant issues/gaps in addressing ML/TF Risk (Counter Measures)

Significant issues/gaps in addressing AML Risk

- ***Identification and verification measures*** Identification and verification measures allow firms to understand who their customer and, where relevant, the beneficial owner is. This is important in that this information forms the basis for ongoing monitoring of the business relationship. It also allows firms to verify that the customer is who they claim to be.

- **Effective Supervisory Oversight**
  Regulatory bodies that oversee the e-payments ecosystem should have a risk based approach in their supervision of such a sector and in addition enforcing the regulatory requirements by all stakeholders.

- ***Methods of funding***
  The ML risk associated with anonymous funding methods can be mitigated by restricting funding methods to sources where providers can rely on another institution´s CDD measures, such as previously identified bank accounts, credit or debit cards or other personalized payment methods

Significant issues/gaps in addressing ML/TF Risk (Counter Measures)

Significant issues/gaps in addressing AML Risk

- **Security in e-payment process-**

  Secured e-payment transaction system is critical to e-business. Without a secured payment trasaction system, e-commerce will be a castle build in the sand. There are two commonly used secure e-payments Secured Socket Layer (SSL) and Secured Electronic Transaction (SET).

- **Awareness and Education-**

  Awareness of security risks by merchants and consumers plays an important role in reducing fraud in e-payments Merchants awareness and education is also important. They should be aware of the types of frauds, statistic and best practices. Consumer awareness and education is important in order to reduce Identity theft or payment data theft.

- ***Methods of funding***

  The ML risk associated with anonymous funding methods can be mitigated by restricting funding methods to sources where providers can rely on another institution´s CDD measures, such as previously identified bank accounts, credit or debit cards or other personalized payment methods

The Way Forward

- Despite all the accounts of fraud, phishing, and hacking, it's hard to deny that digital payment is the future of commerce. Fraudsters will always be present whether online or offline transactions, so abandoning virtual transactions is not the best solution.

- The overall solution is to be aware of today's best and most popular payment gateways and sticking to the one that you are familiar with.

- Educate yourself on the future of online payments and start using solutions that provide data security, contingencies, and dispute opportunities.

CONCLUSION & RECOMMENDATIONS

- ML/FT are serious criminal activities with dire consequences.
- Fighting these crimes requires the collaborative efforts of all stake holders.
- Money laundering, terrorist financing and the related predicate crimes can undermine the stability of a country's financial system or its broader economy in a number of ways. There is therefore the need to kill it before it kills us.
- Throughout the process, one's indiscretion can make him/her an accessory to the crime by way of abetment, conspiracy , negligence, aiding and non-cooperation.
- With the development of e-payment options, the number of online shoppers and merchants keep rising. This has provided fast, reasonably safe and relatively low cost operations for e-business. As the financial and other data is become digitized, the opportunities for e-payment frauds also continues to rise. Furthermore, new fraudulent and sophisticated techniques are being developed by the fraudster. The merchants and the consumers have to be cautious and take preventive measure to minimise the fraud in e-payment transactions.

CONCLUSION & RECOMMENDATIONS

Recommendations:

- General control and security environment of the systems being used should be strengthened
- Specific control and security measures for E-payment methods should be done on case by case basis.
- Customer awareness, education and communication.
- Invest in Top-of the-Range Fraud Detection & Prevention (FDP)Solutions.
- Effective CDD at all levels in the transactions.

E-PAYMENT TRENDS IN GHANA

.

Trends of E-Payment crimes in Ghana.

Fraud cases relating to cyber-crime involved email fraud, crime perpetrated through internet banking and other localized payment and mobile banking platforms. During the year under review Cyber fraud cases decreased by 34.48 per cent from 174 cases in 2018 to 114 cases in 2019. However, despite the decrease in 2019, cyber fraud accounted for the highest value of attempted fraud amounting to GH¢ 50.54 million (9.2 million USD) (with actual loss of GH¢14.31 million (2.6 million USD).

Source: Bank of Ghana.

REFERENCES

- Money Laundering Techniques with Electronic Payment Systems by Krzyszt of WODA
- The Payments Ecosystem: Security Challenges in the 21st Century by Phil Smith III Voltage Security, Inc.
- Digital Payments 2020: The making of $500B ecosystem in India by Boston Consulting Group.
- Bank of Ghana website
- Money Laundering Using New Payment Methods (NPM) by Financial Action Task Force (FATF)

THANK YOU