RISK ,FRAUD AND OPERATIONAL EFFICIENCY OF SWIFT PAYMENT NETWORK

PRESENTED BY:

EJAZ AHMED QADRI

- We are a part of technology driven era of Globalization
- Fintech, Smart block chains, BPO, digitized trading, system generated documents and modern corresponding banking are the part of innovative technologies.
- We cannot survive without adopting these modern technologies
- The SWIFT has also adopted similar approach for updating their worldwide payment system network.

Background

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) was founded in Brussels in 1973 provides a network that enables financial institutions worldwide to send and receive information about financial transactions in a secure, standardized and reliable environment. SWIFT also sells software and services to financial institutions, much of it for use on the SWIFTNet network, and ISO 9362. Business Identifier Codes (BICs, previously Bank Identifier Codes) are popularly known as "SWIFT codes". MT' stands for 'Message Type' – the SWIFT network uses a range of Message Types numbered from MT 100 to MT 999 to effect different types of payment orders.

- As of 2018, around half of all high-value cross-border payments worldwide used the SWIFT network. SWIFT transports financial messages in a highly secure way but does not hold accounts for its members and does not perform any form of clearing or settlement.
- SWIFT has been criticized for its inefficiency, with the Financial Times observing in 2018 that transfers frequently "pass through multiple banks before reaching their final destination, making them time-consuming, costly and lacking transparency on how much money will arrive at the other end . so ”SWIFT has introduced its own improved service, called "Global Payments Innovation" (GPI), which details are follow,

EFFICIENCY OF SWIFT PAYMENT NETWORK

SWIFT Launches Customizable Fraud Prevention Service

- SWIFT launched a real-time payment controls services that is designed to strengthen fraud controls. The new fraud and cyber-crime prevention service, which is a part of the company's "Customer Security Program," will enable users to customize how they screen their payment messages.
- Criminals tried to steal $1 billion USD from Bangladesh Bank in Dhaka and managed to walk away with $81 million USD, according to reports.
- On top of other incidents, including $12 million taken from Ecuador's Banco del Austro and an attempted theft stopped by Tien Phong Bank in Vietnam, this major heist led industry experts to increasingly begin questioning whether SWIFT was doing enough to protect the banks in its network.

- SWIFT believes that users having this ability at their controls will allow them to more easily detect any unusual situations before funds are transmitted. The theory is that the users themselves are the ones who best understand the day-to-day transaction patterns in their own operations. So on top of using automated fraud prevention systems and SWIFT's "daily validation reports" tool; they will be the ones who can best identify any irregularities that surface.
- SWIFT listed the following benefits of the new offering:

• Controls which payment instructions you send, providing business assurance to counterparts
• Aligns controls to risks, in support of regulatory guidance
• Rapidly adapts to changing needs and emerging business threats
• Provides primary control point or secondary safety net
• Mitigates regulatory and reputational risk

- **Global Payment Innovation GPI is the new standard.**

- The advent of real-time domestic payments and 24/7 central bank settlement heralded a new dawn for cross-border payments, enabling the industry to re-conceptualise cross-border payments. In 2017 SWIFT and its community moved fast to deliver on this, introducing the 'global payments innovation', or GPI, a new convention based on new technologies. Just two years since launch, gpi is widely embraced by the community and fast proving to be the catalyst for unprecedented change in cross-border payments.

- **Swift gpi transferred $77 trillion in 2019**
- Almost doubling the $40 trillion transferred in 2018, Swift's transmission of $77 trillion in cross-border payments messages over the gpi platform during 2019 implies that demand for the program is becoming entrenched in the bank-to-bank space.
- There are a number of gpi features, which help protect institutions against payments fraud. The gpi Tracker provides the precise location of a payment, giving complete visibility to financial institutions' operations teams who can detect fraud faster by tracking a payment along its journey.
- It's fast - over 50% of gpi payments are credited to end beneficiaries within 30 minutes, 40% in under five minutes, and almost 100% of gpi payments are credited within 24 hours.

- SWIFT and its community created gpi setting three key foundation stones.
- Firstly, the introduction of a humble tag – a unique transaction identifier which accompanies every payment throughout its trajectory. The existence of this 36-character marker (The Unique End-to-End Transaction Reference, UETR) allows payments to be traced as they go from originating senders, through correspondents, to ultimate beneficiary accounts.
- Secondly, the introduction of a tracker which follows these payments along their trajectory and reports back on their status, on demand.
- Thirdly, the establishment of a new cross-border convention under which banks commit to process payments from ordering customer right through to end beneficiary within tight timeframes – timeframes that are made visible to their respondents and correspondents,

- **Major trade banks are digitizing trade on SWIFT**

- SWIFT is leveraging an extensive platform connectivity to digitize Letter of Credit (LC) presentation, delivering new efficiencies and removing friction from global trade. In the complex world of documentary trade finance, digital communication has the power to deliver greater efficiencies, an enhanced user experience, and long-term growth in global trade. As the industry continues to look for ways to mitigate the notorious paper burden in documentary trade, SWIFT and a group of leading banks embarked on an initial Proof of Value (PoV) to explore how current trade processes could be digitized by leveraging and unlocking the power of the SWIFT network

- **Digitizing processes to increase efficiency;** during the first phase of the project, four banks successfully tested the SWIFT solution internally. DBS and J.P. Morgan went on to conduct successful external trials, resulting in a 30 per cent reduction in paper from documentary trade.

- They are constantly exploring new solutions and partnerships to work towards a future of frictionless trade. This is another initiative that complements overall efforts in dematerializing trade documents and simplifying the manual and complex letter of credit process.

Alternatives

- Besides that, perception is also there that SWIFT has monopolistic and under influenced of big economic powers, so many countries or regions are thinking otherwise and alternative payment network are there .e.g.,

- Russia, China & India to set up alternative to SWIFT payment system to connect 3 billion people

- Members of the BRICS trade bloc Russia, India, and China have decided to connect their financial messaging systems to bypass the SWIFT international money transfer network. Russia's financial messaging system SPFS ('System for Transfer of Financial Messages') is a Russian equivalent of the SWIFT financial transfer system, developed by the Central Bank of Russia. ... SPFS accounts now around 15% of all internal trafficking inside Russia will be linked with the Chinese **cross-border interbank payment system CIPS**.

While India does not have a domestic financial messaging system yet, it plans to combine the Central Bank of Russia's platform with a domestic service that is in development.

- The new system is expected to work as a "gateway" model when messages on payments are transcoded in accordance with a certain financial system.
- Russia & Iran to switch to SWIFT-free banking system
- Instead of SWIFT, two countries will use their own domestically developed financial messaging systems – Iran's SEPAM and Russia's SPFS.
- Using this system for trade and business exchanges between EAEU [Eurasian Economic Union] member states (The Eurasian Economic Union includes Armenia, Belarus, Kazakhstan, Kyrgyzstan and Russia.) can help develop and expand trade exchanges between the member states as well.

RISK & FRAUD IN SWIFT PAYMENT NETWORK

SWIFT Fraud on the Rise: According to a new report ("How Banks Are Combating the Rise in SWIFT Cyber Fraud") from EastNets, the problem of SWIFT fraud may be more widespread and dangerous than originally thought. In the aftermath of the epic $81 million SWIFT fraud attack on Bangladesh Bank in 2016, the SWIFT interbank messaging platform immediately put new safeguards in place in order to neutralize risk. However, EastNets surveyed 200 banks worldwide and found that 4 in 5 of these banks had experienced at least one SWIFT fraud attempt since 2016, and the problem appears to be growing on an annual basis.

Key findings on SWIFT fraud

- Despite this spike in SWIFT cybercrime activity, most banks and financial services providers are taking a hands-off approach to dealing with this problem. According to the EastNets report, a "significant portion" of the banks surveyed said that they still did not have prevention policies in place to address SWIFT fraud? In many ways, they appear to be relying on the SWIFT network to do all the heavy lifting
- One problem, says EastNets, is that "insider risk" is on the rise. In other words, hackers on the outside are combining forces with employees at banks in charge of sending or receiving SWIFT payments in order to approve certain financial transactions or to override any red flag signals the security system might be generating. According to the SWIFT fraud report, 1 in 7 banks have experienced at least one SWIFT fraud attempt involving an employee.

- While the problem of SWIFT fraud is worldwide, the problem appears to be particularly acute in the Asia-Pacific region. This, of course, was the region where the epic Bangladesh Central Bank fraud took place (which involved accounts the bank had the Federal Reserve Bank of New York). Asia is also a prime destination for “beneficiary accounts” linked to hackers. Of the money stolen from the SWIFT network, 83% is forwarded to beneficiary accounts in Asia, and 10% to Europe. Moreover, the risks involving banks in Asia-Pacific are highlighted by the fact that almost 100% of banks and financial services providers in the Asia-Pacific region using the SWIFT payment network have been victimized at least once by SWIFT fraud. In other words, it’s not a matter of “if” SWIFT fraud is going to occur in Asia, but “when.”

- **An example of spoofing** (is when an email is sent from a false sender address that asks the recipient to provide sensitive data.)This email could also contain a link to a malicious website that contains malware.
- The announcement around the Bangladesh bank hack said that there had been a number of fraudulent messages, and warned their members to update their software (by 12 May 2016), as the hack involved modifying Swift's software on back office computers within the Bangladesh central bank, in order to hide the transaction.
- It is thought that the intruders obtained valid operator credentials using a "spoofed" ID, and which can create and approve Swift messages. They then submitted fraudulent messages based on the identity of those they are spoofing.

Swift 103 Fraud

One of the biggest industry scams are Swift Mt103 Fraud transactions, specifically:

- Swift Mt103/23
- Swift Mt103 One Way (Mt103/202)
- Swift Mt103 Two Way

Swift Mt103 History

The Mt103 is a simple form of SWIFT message that is commonly used by banks to perform the movement of funds from the sender's bank to the beneficiary's bank. The Mt103 is a vanilla SWIFT Message that only allows very basic terms to be attached to the SWIFT Mt103 transfer. These terms normally cover things such as the beneficiaries bank undertaking to advise the beneficiary that the transfer has been completed.

Mt103/23 - The Sender Scam

- Scammers con people into believing that there is such a thing as a "conditional" Mt103 named an Mt103/23. They claim that with a "conditional" Mt103/23 the beneficiary's bank will not release the funds to the beneficiaries account until the beneficiary completes specific documents or the sender has provided confirmation that the funds can be released by the Beneficiaries bank to the beneficiary.
- The truth is..... The Mt103 is NOT designed for ANY type of conditional transaction and you CANNOT send a Mt103 or a Mt103/23 with any type of condition attached!

- The Field 23 Instruction Code used to be used where the sending bank (at the request of the sender) puts a simple code instructing the beneficiary's bank how to effect payment. Field 23 is VERY LIMITED and is designed solely for basis short text like: "Telephone Beneficiary on Receipt" or "Credit Account Immediately". There was no space to enter "conditions". So there was NO POSSIBLE WAY to send an Mt103/23 or an Mt103 with any type of "condition"
- Transactions that involve the conditional release of documents are administered by lawyers, escrow and trustees, NOT BY BANKS!
- Today Field 23 is **no longer used** and any reference to a Mt103/23 is false. That field is now defunct and no longer used by ANY Bank. Today any person offering you a Mt103/23 transaction is committing fraud by offering an impossible transaction that has no technical way of ever being keyed into the SWIFT System.

- **Mt103 One Way - The Receiver Scam**

- **Mt103 Two Way - The Receiver & Sender Scam**

- In this scam customers are told they just need to have a bank account to receive a 30 Million dollar Mt103, when they receive the 30 Million Dollar Mt103 payment, the customer is allowed to keep 5 Million Dollars and then he needs to wire the other 25 Million Dollars to bank coordinates that are provided to him by the scammer. Yes you get 5 Million dollars for **receiving stolen funds, being a part in a Money laundering chain and paying the 25 Million of stolen money to a new clean account as you are instructed by a person you have never seen and never met.**

- The problem is when the Police finally get around to investigating the stolen funds and cash, they trace the SWIFT Mt103 right to your account.
- You then have two options repay the 30 million dollars that was stolen or go to jail. Judges in these cases have been particularly harsh with "innocent receivers" who claim they knew nothing about the fraud but were happy to bank a 5 million dollar profit for letting the funds pass through their account.
- **Letter of Credit Fraud**
- Legitimate letters of credit are never sold or offered as investments. They are issued by banks to ensure payment for goods shipped in connection with international trade. Payment on a letter of credit generally requires that the paying bank receive documentation certifying that the goods ordered have been shipped and are en route to their intended destination.

- Letters of credit frauds are often attempted against banks by providing false documentation to show that goods were shipped when, in fact, no goods or inferior goods were shipped.

- Other letter of credit frauds occur when con artists or cheaters offer a “letter of credit” or “bank guarantee” as an investment wherein the investor is promised huge interest rates on the order of 100 to 300 percent annually. Such investment “opportunities” simply do not exist.

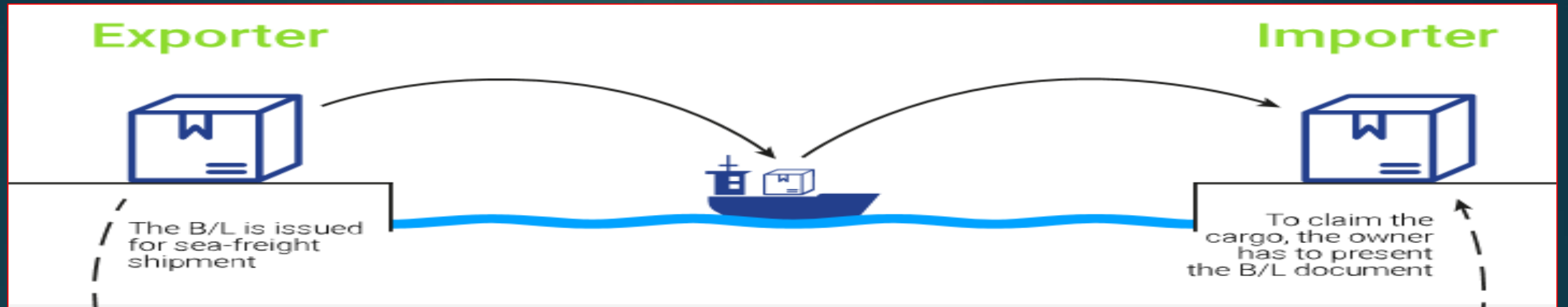
Smart B/L Block chain-Based Bill of Lading (B/L) Documents for Global Trade

The global logistics industry is introducing Smart B/L documents based on block chain technology, replacing old-style paper Bill of Lading documents. With the Smart B/L users will be able to state and transfer cargo ownership rights without the hassle of handling paper. The shipping industry still uses paper for issuing proof of cargo ownership. Blockchain and Smart Contracts are made for this industry.

- Secure; No central storage, which could be attacked by hackers. Global Trade's most important document is encrypted and securely written on the block chain network, accessible only with traders' private keys
- Fast; Smart B/L is issued instantly and is immediately available to the Exporter. When agreed conditions are met, Smart B/L is transferred to the legal owner of goods – instantly, without couriers in the middle. Just like sending an e-mail

- Paperless; A blockchain-based Smart B/L will be equivalent to a paper one. Having it on the blockchain just takes the pain away. No need to print, send, store and archive it in a conventional way anymore.
- Cost savings; Each paper B/L is sent at least three times with couriers making it extremely expensive and slow. The average cost for sending a B/L three times is around $100 and it takes up to 10 days to reach the final destination. More than 50 million B/Ls are created per year.

- A Blockchain is a ledger that uses cryptography, the internet and naturally computers to create, share, transfer, track and secure assets and transactions (represented/organised as blocks) belonging to everyone to fulfil a certain function..
- Unless the previous transaction is completed in the chain and shared forward with a timestamp, the next transaction cannot happen..” A very generic and basic pictorial of the Blockchain is as below..



Transfer of B/L ownership

Old way

The total time needed for B/L transfer via express courier service:

5-10 days

New way

Blockchain based token - Smart B/L

The total time needed for B/L transfer via blockchain and dApp:

20s

Q & A

Thank You!