UNODC
United Nations Office on Drugs and Crime

POIDN Alert No. 1/2017

GROWING THREAT OF ELECTRONIC MONEY LAUNDERING AND TERRORISM FINANCING

This alert is aimed to raise awareness on the use of magnetic-stripe cards as money laundering and terrorism financing tools.

Key messages

- Although Prepaid cards are not widely circulated in Indonesia, their use in the country cannot be ignored as they can be obtained externally.
- Magnetic-stripe products are increasingly being used as electronic money laundering tools.
- Funds can be transferred to be used for financing terrorism.
- The industry and law enforcement agencies should detect, investigate, and prosecute the fraudulent activity often associated with prepaid cards and other magnetic-stripe products.

The United Nations Office on Drugs and Crime (UNODC) supports member states to strengthen their ability to implement measures to counter money laundering and the financing of terrorism through means that detect, seize and confiscate illicit proceeds as required in relevant United Nations instruments. These instruments are bolstered by the 1998 Political Declaration and measures for countering money laundering adopted by the UN General Assembly at the Twentieth Special Session.

UNODC Indonesia carries out this mandate under its current regional and Country programmes and has supported the relevant institutions to address issues such as corruption, money laundering and financing of terrorism. As part of this continued support, UNODC shares information that can be used to strengthen the capacity of law enforcement and the wider criminal justice system to combat these threats. The purpose of this Alert is to raise awareness on the use of prepaid and other magnetic-stripe products as a money laundering tool. Law Enforcement agencies should be aware that there is a myriad of other illicit activities that can be facilitated with the use of these cards (e.g. terror financing).

RECENT THREATS

The emergence of the use of prepaid cards and other magnetic-stripe products to hide illicit proceeds, launder money and to fund acts of terror, is a growing threat. This was evident in a act of terror in 2016 where perpetrators used prepaid credit cards rather than cash transfers to transfer funds to support the operation. Unfortunately, many of the same features that make prepaid cards a positive payment innovation have also attracted criminals interested in exploiting this electronic money form to facilitate money laundering and other illicit activities.

In Indonesia, the use of New Payment Method (NPM) on money laundering that includes Prepaid Cards, and Mobile Payments in financial transactions, is growing rapidly. NPM leads to increased risk which can be used in various cases of fraud. However, in its development, NPM is known to be one of the alternative payment methods used in gambling, especially online gambling. Based on a national risk assessment carried out by PPATK (Indonesia's FIU), it is known that the financial tools at high risk include the transfer of funds of terrorism via electronic payment systems, online payment systems, or new payment methods, through prepaid cards, and foreign currency exchange activities as well as through cash both domestically from abroad by terrorist networks (couriers).

Prepaid cards comes in two types – Closed and Open system cards. Closed system cards include gift and phone cards and although they have some limitations, they can be a viable vehicle to move money undetected. On the other hand, Open system cards pose a more significant money laundering threat as these cards are usually branded by

American Express, MasterCard and Visa and operate like regular credit or debit cards.

There have also been cases of criminals reprogramming and using the magnetic-stripes of prepaid cards, gym cards, hotel card keys and other nondescript products to store and disguise illicit funds. Other related actions by criminals include:

- Criminals compromising victim account information through phishing, database hacking, or through skimming at bars, restaurants, gas pumps or ATMs.
- The account information is re-encoded onto the magnetic-stripe of the prepaid access card, which is purchased or stolen from non-secure store displays. (Cards may also be purchased online)
- Sophisticated fraudsters will wash the face of the prepaid access card with a solvent to dissolve the printed card numbers, and then emboss any name of their choosing and new numbers into the plastic, giving the gift card the appearance of a traditional credit or debit card complete with security features.
- Criminals now have the ability to hold thousands of dollars on the magnetic-stripes of prepaid cards.

These instruments create enormous challenges for law enforcement as they serve as valuable means to launder funds, finance terrorism or move large amounts of cash without detection by legal mechanisms. Features of these include:

- The global nature of funding
- Absence of set maximum limits to card balances
- Option for use at ATM's as credit cards
- No requirement for bank accounts
- Online activation

Although it might be tedious to purchase prepaid access cards in bulk, criminals have been known to spread their purchases among several different retailers, often using groups of mules to purchase the cards and avoid detection. These cards are also a convenient vehicle to aggregate and transport funds, as a person carrying multiple cards is typically not a cause for alarm. From a law enforcement perspective, few officers have the ability or authority to determine a prepaid cards actual value, should they come across suspicious activity or individuals. Therefore, it is critical that the Government of Indonesia adopts measures to equip law enforcement institutions to counter the use of these cards.

INVESTIGATIVE CHALLENGES AND RESPONSES

Prepaid access cards often look and transact just like traditional credit and debit cards. They are also easier to obtain than traditional cards. While these traits make prepaid access cards popular among consumers and retailers, they also make it difficult for the industry and law enforcement agencies to detect, investigate, and prosecute fraudulent activity associated with them. Some of these challenges include:

- Lack of training or incentive for retail staff to detect and report incidents involving compromised accounts or cards.
- Insufficient detection equipment and training provided to local law enforcement officers to identify and process corresponding evidence.
- Lack of supervision of the use of prepaid cards that tend to weaken the function of identification "Know Your Customer"

Given these challenges, institutions, law enforcement, and prosecutors must work together to share information, expertise and tactics through participation in public-private groups such as the International Association of Financial Crimes Investigators (IAFCI).

While prevention is key, one future consideration to minimize prepaid access card abuse may include securing products away from public handling prior to sale. The ability to isolate certain account use by authorizing only certain purchases (i.e., over computer only or via telephone only) with incorporated logarithms might inhibit some abuses when facilitating online purchases. In addition, persons in the best position to detect fraudulent activity, (frequently a retail sales associate) should be trained to deter or interdict the crime.

For further Information, please contact:
UNODC Indonesia
Menara Thamrin, Jl. MH. Thamrin Kav. 3
Jakarta 10250
Phone: (021) 29802300
Fax: (021) 3145251

Visit us on https://www.unodc.org/indonesia/

Follow us **@UNODC_POIDN**

Like our FB Page
https://www.facebook.com/unodc.id/