Webinar

13 May 2020 | 09:00 am GMT [LIVE]

Impact of COVID-19 on Financial Crimes

YOU Jung Kee

Muhammad IMRAN

INTERPOL

Impact of COVID-19 on Financial Crimes

- INTERPOL Financial Crimes Unit
- Crime typologies emerging from COVID-19
- Looking ahead
- Recommendations for law enforcement

A GLOBAL STRUCTURE

Financial Crimes Unit (FCU)





- Based in Lyon, Bangkok & Singapore

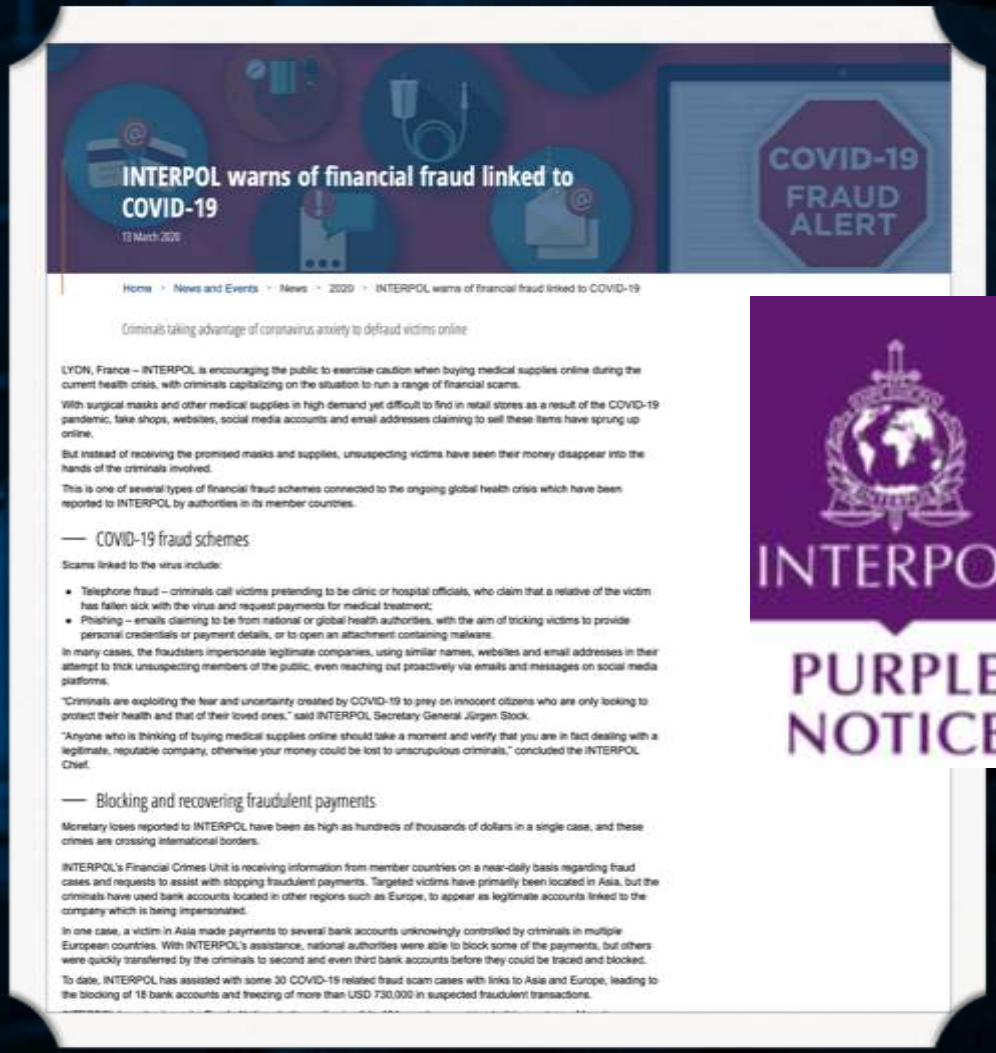
- Bridge multiple jurisdictions to combat transnational financial crimes 24/7
- Sends alert on latest crimes and crime trends





Alert new crimes – warns of fraud linked to COVID-19

https://www.interpol.int/News-and-Events/News/2020/Unmasked-International-COVID-19-fraud-exposed



INTERPOL warns of financial fraud linked to COVID-19

13 March 2020

COVID-19 FRAUD ALERT

Home › News and Events › News › 2020 › INTERPOL warns of financial fraud linked to COVID-19

Criminals taking advantage of coronavirus anxiety to defraud victims online

LYON, France – INTERPOL is encouraging the public to exercise caution when buying medical supplies online during the current health crisis, with criminals capitalizing on the situation to run a range of financial scams.

With surgical masks and other medical supplies in high demand yet difficult to find in retail stores as a result of the COVID-19 pandemic, fake shops, websites, social media accounts and email addresses claiming to sell these items have sprung up online.

But instead of receiving the promised masks and supplies, unsuspecting victims have seen their money disappear into the hands of the criminals involved.

This is one of several types of financial fraud schemes connected to the ongoing global health crisis which have been reported to INTERPOL by authorities in its member countries.

COVID-19 fraud schemes

Scams linked to the virus include:

- Telephone fraud – criminals call victims pretending to be clinic or hospital officials, who claim that a relative of the victim has fallen sick with the virus and request payments for medical treatment;
- Phishing – emails claiming to be from national or global health authorities, with the aim of tricking victims to provide personal credentials or payment details, or to open an attachment containing malware.

In many cases, the fraudsters impersonate legitimate companies, using similar names, websites and email addresses in their attempt to trick unsuspecting members of the public, even reaching out proactively via emails and messages on social media platforms.

"Criminals are exploiting the fear and uncertainty created by COVID-19 to prey on innocent citizens who are only looking to protect their health and that of their loved ones," said INTERPOL Secretary General Jürgen Stock.

"Anyone who is thinking of buying medical supplies online should take a moment and verify that you are in fact dealing with a legitimate, reputable company, otherwise your money could be lost to unscrupulous criminals," concluded the INTERPOL Chief.

Blocking and recovering fraudulent payments

Monetary loses reported to INTERPOL have been as high as hundreds of thousands of dollars in a single case, and these crimes are crossing international borders.

INTERPOL's Financial Crimes Unit is receiving information from member countries on a near-daily basis regarding fraud cases and requests to assist with stopping fraudulent payments. Targeted victims have primarily been located in Asia, but the criminals have used bank accounts located in other regions such as Europe, to appear as legitimate accounts linked to the company which is being impersonated.

In one case, a victim in Asia made payments to several bank accounts unknowingly controlled by criminals in multiple European countries. With INTERPOL's assistance, national authorities were able to block some of the payments, but others were quickly transferred by the criminals to second and even third bank accounts before they could be traced and blocked.

To date, INTERPOL has assisted with some 30 COVID-19 related fraud scam cases with links to Asia and Europe, leading to the blocking of 18 bank accounts and freezing of more than USD 730,000 in suspected fraudulent transactions.

INTERPOL PURPLE NOTICE

Crime typologies emerging from COVID-19

Modi Operandi reported from member countries during the pandemic era

1. Advanced payment fraud
2. Donation fraud
3. Telephone fraud / Phishing
4. Vaccine & Testing kit fraud
5. Business Email Compromise (BEC) fraud

Crime typologies emerging from COVID-19

1. Advanced Payment Fraud

Recommendations

Be vigilant.
Be skeptical.
Be safe.

www.interpol.int vs www.interp**0**l.int

me@interpol.int vs me@**1**nterpol.int

- Domain age
- Poor grammar
- Video call & check product

Crime typologies emerging from COVID-19

2. Donation Fraud

"Please show your generosity"

"Help this organization to save COVID-19 patients"

"Let's send masks to front-line helpers who need the most"

"Cryptocurrency payment available"

Recommendations

Be vigilant.
Be skeptical.
Be safe.

www.interpol.int vs www.interp0l.int

Where you've donated before, in the same way you did.

Put web address into the address bar. Do not click on shortcut links.

Crime typologies emerging from COVID-19

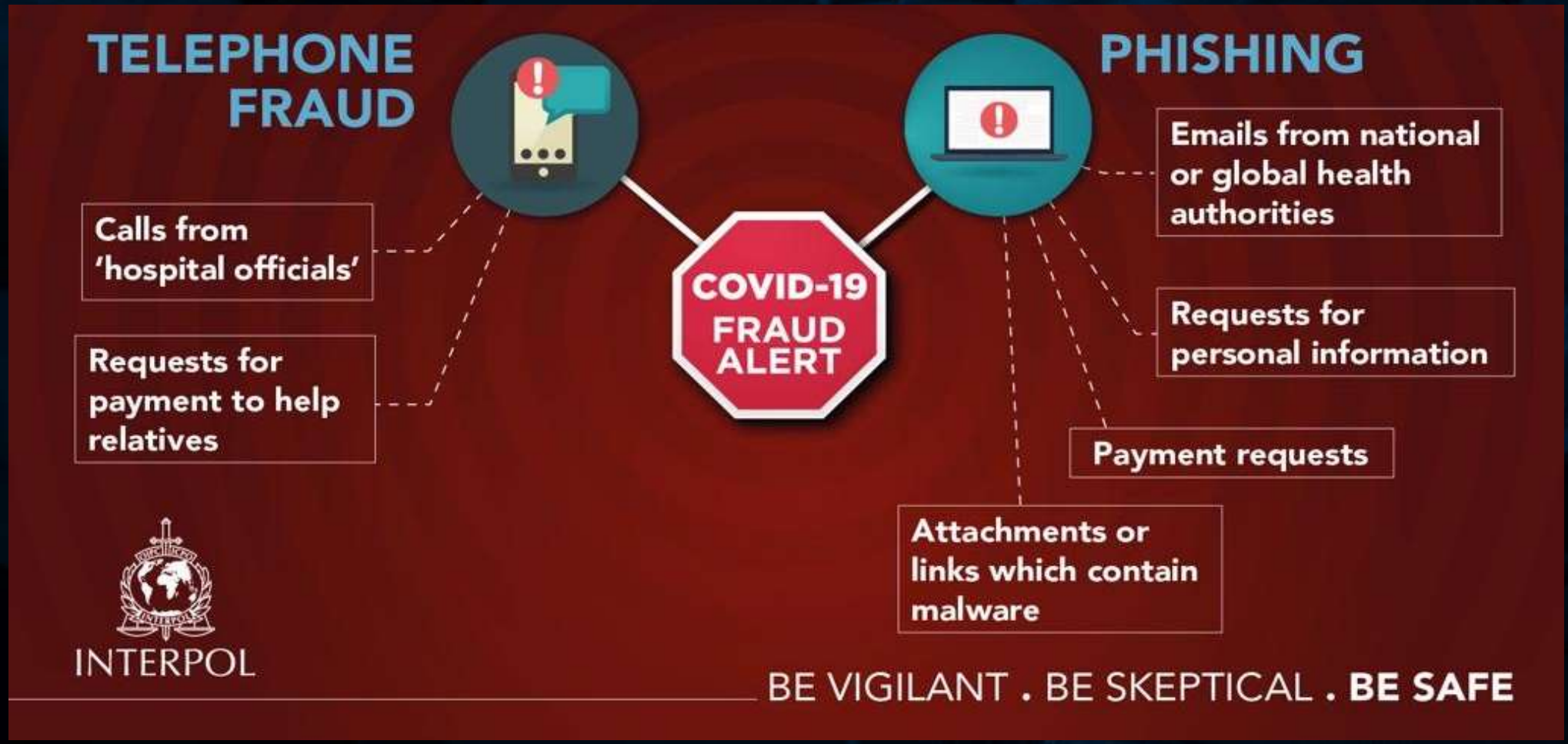
3. Telephone fraud / Phishing

Department of Health officer: “I require your details to conduct contact tracing”

Dr X: “Please pay the costs of the medical treatment for your relative/grandchild”

INTERPOL

Case Study



Recommendations

Be vigilant.
Be skeptical.
Be safe.

- Never divulge personal details to anyone
- Always reverify with the authorities using another mode of communication
- Take note that phone numbers & email addresses can be spoofed

Crime typologies emerging from COVID-19

4. Vaccine & Testing Kit Fraud

"We are exporting testing kits for COVID-19."

"We have finally invented the vaccine for COVID-19!"

INTERPOL

Case study

Recommendations

Be vigilant.
Be skeptical.
Be safe.

- Vaccines are not available for now
- Buy products from reputable companies or those endorsed by the authorities
- Be wary of fake brands and investment fraud

Crime typologies emerging from COVID-19

5. Business Email Compromise (BEC)

“Due to the pandemic, transactions have to be made to a new account from now on”

"Product related to COVID-19 is in demand all over the world. Act quickly!”

INTERPOL

THE ANATOMY OF BUSINESS EMAIL COMPROMISE

3 TOXIC INGREDIENTS

Low cost!
Low risk!
High rate of return!

= **Millions in illegal profits**

1 Hacking

An email account is compromised through malware, employee intrusion, etc.

2 Social engineering fraud

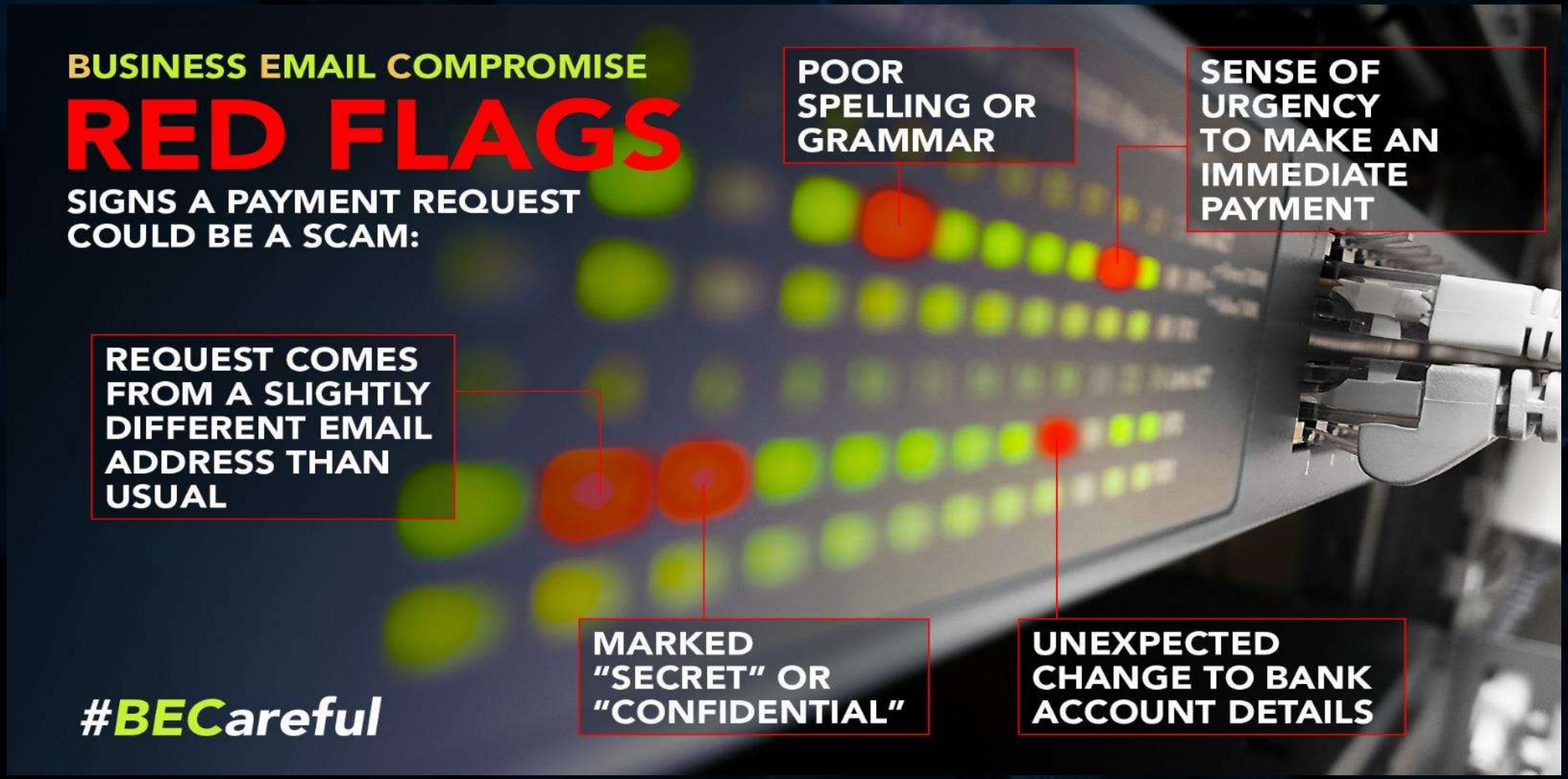
The victim is manipulated into providing information or funds.

3 Money laundering

Multiple transfers are made involving foreign banks/ institutions

#BECareful

Recommendations



Recommendations

Looking Ahead

Advanced payment fraud

Donation fraud

Telephone fraud / Phishing

Vaccine & Testing kit fraud

BEC fraud

Cybercrimes

Loan-related crimes

Money mule

Investment fraud

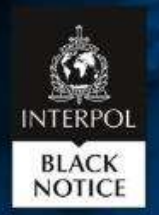
INTERPOL

INTERPOL NOTICES

RED NOTICE
WANTED PERSONS

YELLOW NOTICE
MISSING PERSONS

BLUE NOTICE
ADDITIONAL INFORMATION



BLACK NOTICE
UNIDENTIFIED BODIES

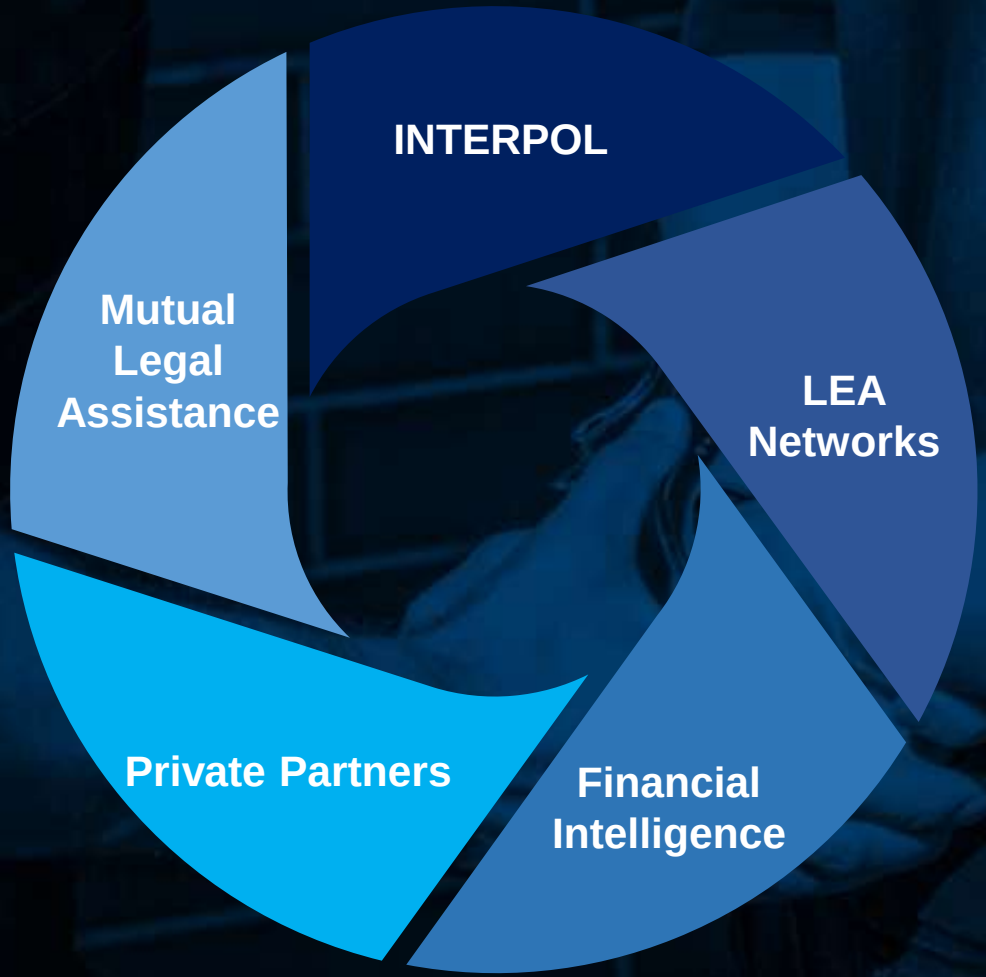
GREEN NOTICE
WARNINGS AND INTELLIGENCE

ORANGE NOTICE
IMMINENT THREAT

PURPLE NOTICE
MODUS OPERANDI

INTERPOL–UN SECURITY COUNCIL SPECIAL NOTICE:
GROUPS AND INDIVIDUALS SUBJECT TO UNSC SANCTIONS

Continuous Efforts for International Cooperation



OEC-CNET-FCU@interpol.int