STATEMENT BY
MRS. ANDREA MARTIN-SWABY
DEPUTY DIRECTOR OF PUBLIC PROSECUTIONS AND HEAD OF JAMAICA'S CYBERCRIMES AND DIGITAL FORENSICS UNIT

ON BEHALF OF

THE CARIBBEAN COMMUNITY

(CARICOM)

AGENDA ITEM 4: PROVISIONS ON CRIMINALIZATION

PLENARY (ROOM M-3)

JUNE 1, 2022

Thank you Madame Chair,

CARICOM seeks to address the second set of questions which have been posed in relation to the provisions for the Chapter on Criminalization.

CHAIR'S SECOND GROUP OF QUESTIONS – B COMPUTER RELATED FRAUD & FORGERY

1. Do you think that the offence of fraud, committed in whole or in part online, is sufficient to cover other conducts such as theft, scam, financial offences, and electronic payment tools offences?

2. Regarding computer/ICT-related forgery, what kinds of [mental/fault] elements (for example [malicious/dishonest] intent) should be included in the criminalization of such act? Should the convention consider putting in place legal protections for cybersecurity researchers and other professionals working in cybersecurity (including, inter alia, penetration testers)?

3. Could we consider the proposed provisions on "creation and use of digital information to mislead the user", as a form of [computer] [ICT]-related forgery?

4. How do you think the convention should deal with identity-related offences?

Computer Related Fraud & Forgery -

Madame Chair,

CARICOM has considered traditional criminal offences which may already be covered by domestic law in the countries of our region and other international instruments, but which are also frequently committed through the use of computer systems or information and communication technologies.

CARICOM submits that Forgery and Fraud are examples of offences in which the use of computer systems change the scope and impact of these crimes. Member States are encouraged to

favourably consider the inclusion of these offences in the Convention.

CARICOM acknowledges that most States may have previously criminalized these activities at the domestic level but may not have addressed these activities when they are committed through the use of a computer system or information and communication technology.

In light of the peculiar nature of these offences, and the fact that they may be otherwise covered, States Parties may conduct their own legislative analysis and determine whether there is a need to enact new provisions or amend existing ones, or leave intact their current law if they are deemed to be sufficient to cover these offences.

On this basis, CARICOM recommends the inclusion within the new convention of these specific cyber enabled crimes:

1. Fraud perpetrated by the use of ICT's
2. Forgery or falsification of computer material or data.

Traditionally, the offence of forgery consisted of the falsification of tangible documents and not intangible data. The laws concerning this offence were almost incapable of addressing the alteration, suppression, deletion, manipulation or misrepresentation of data. It therefore posed a serious challenge for prosecution as well as for stakeholders.

Madame Chair

Forgery is a type of fraud which can be perpetrated without the falsification of a tangible document. The alteration, deletion, manipulation and suppression of data is a forgery of data where the intention is to mislead a person into believing that the data is accurate. The technological era has created innovative ways of committing this traditional offence which changes the scope of the act. CARICOM believes that the use of computer changes the scope of this traditional crime. The future-proofing of a new

convention ought to address the evolving nature of such crimes using ICTs.

Madame Chair,

A fraud in its purest sense, consists of a dishonest act whether through deceit, falsehood or other forms of dishonest or fraudulent means. Where such an act is committed, there is a deprivation caused by the act which may consist of an actual loss for the victim or the endangerment of the victim's financial interests. In such circumstances, where a fraud is perpetrated, the law does not require that the person who perpetrates the fraud has benefited from it for culpability to arise and the victim does not have to suffer an actual or material loss as a result of the fraud.

A computer related fraud exists where the intentional dishonest act is perpetrated through the manipulation, suppression, alteration or deletion of data. Where such an act is done with the intention to procure an advantage and causes deprivation, it is a fraud facilitated through technological means.

The Act & The Mental Element – FRAUD

The mens rea "mental element" for fraud without the use of ICT consists of the accused subjective knowledge that the act was dishonest and that it could cause a deprivation for a third party

CARICOM proposes that the same mental element required to prove a traditional fraud perpetrated without the use of ICT's, apply to a fraud involving the use of ICT's. This will ensure consistency in legislation within the domestic context.

MADAME CHAIR,

Mental Element – Computer Related Forgery

CARICOM further proposes that the mental element required for forgery using ICTs should be similar to the mental element which is required for Fraud using ICT, where there is a requirement for the act to be intentional and not reckless or the other lower forms of mens rea such as (negligence).

Madame Chair, you have asked whether Member States are of the view that the offence of fraud committed in whole or in part online, is capable of covering conducts such as theft, scam, financial offences and electronic payment tools offences.

CARICOM believes that if the language we have recommended for this article is adopted then it will offer the widest possible scope of applicability to the varying forms of fraudulent activities.

We explored the traditional offence of fraud. The offence of Fraud takes many forms in the traditional space. Yet, the wide definition of the actus reus of fraud as outlined above is a good foundation for addressing the dishonest act, irrespective of the medium through which the fraud was perpetrated.

In addressing frauds which are perpetrated in the digital space, CARICOM recommended that the constituent elements are "input, alteration, deletion, and suppression of data". These words are arguably capable of addressing the categories highlighted by the Chair.

Madame Chair, you have also asked whether the creation and use of digital information to mislead the user would be a form of computer related forgery.

CARICOM posits that the creation and use of data to mislead may be aptly captured as forgery. Further, where it is done for the purpose of obtaining a benefit and causes deprivation, it would also qualify as a computer related fraud.

MADAME CHAIR,

Identity Related Crimes -

CARICOM submits that "identity related crimes which are sometimes classified as "identity theft" are arguably variations of forms of fraudulent activity. These involve in many instances manipulation, falsification and possible manipulation of data for the purpose of obtaining a benefit or gaining an advantage whilst also causing deprivation.

In the case of identity related crimes, computers, networks and processed information are being used to commit the traditional crime of fraud and/or forgery. CARICOM opines that the broad terms of the Article within the instrument may be apt to cover most instances of identity related offences. However, we have observed that in several countries, specific legislative provisions have been enacted to address "Identity Related" crimes within their domestic law.

In concluding, Madame Chair, CARICOM posits that this area of the law is one which Member States may consider carefully whether the instrument needs specifically to cover this offence or whether Member States can be given the flexibility to criminalize specific identity related offences.