

Modern Law for Global Commerce

Congress to celebrate the fortieth annual session of UNCITRAL
Vienna, 9-12 July 2007

Cybercrime and Commercial Fraud: A Nigerian Perspective

By Nuhu Ribadu
Executive Chairman,
Economic and Financial Crimes Commission, EFCC, Nigeria

I feel greatly privileged and appreciative for the kind invitation to be in your midst for this very important event. As you all probably are already aware, I head the Nigerian law enforcement organization we call **The EFCC** that specializes in the investigation and prosecution of financial and economic crimes and which was created in the year 2004, in part, as a major response to offences that international law has today characterized as cybercrime.

Although we operate, regarding all cybercrime offences, on the basis of a Parliamentary Act called the Advance Fee Fraud and other Offences Act of 2006, Cybercrime laws, in the best of circumstances, function best within the framework of a clearly dedicated law and not as an appendage that allows remedies to fall short of liabilities. I will speak a little more on this later in my presentation.

In its import and practice, the law deals with offences that fall within the ambit of section 419 of our Criminal Law Act which deals with the offences of obtaining by false pretence through different fraudulent schemes such as contract scam, credit card scam, inheritance scam, job scam, lottery scam, currency scam, marriage scam, immigration scam, counterfeiting, religious scam as well as cases of cyber crime. For years now, businesses, learning institutions, and government departments have been receiving e-mails from senders posing as Nigerian/West-African government or business officials offering to share large sums of money. So pervasive is this scam that we have a dedicated section led by some of our best operatives to investigate and prosecute these crimes. However as you can see from what I have described so far, it does not embrace the robust framework of what the Council of Europe has distilled so clearly in its 2001 Budapest Convention on Cybercrime. Let me say however in passing that we are currently in consultation with sister nations in our sub-region with a view of coming up with a clear regional statute regarding cybercrime and we welcome partnership and collaboration with the UNCITRAL in this effort.

Having said that much, I must say here that cybercrime in the manifestation that other parts of the world understand it also manifest itself in Nigeria, perhaps more than any other African nation today. Our AFF team members therefore deal with myriad offences under its omnibus cybercrime definition that straddle matters of data interference, system interference, illegal interception, illegal access and the misuse of devices in the very typology derived from the characterization of the Council of Europe.

The truth is that cybercrime is depressing trade and investor confidence in our economy and to that extent it is a present and clear danger to our national security and the prosperity of our citizens. In deed of all the grand corruption perpetrated daily in our communities, most are of the nature of cybercrime executed through the agencies of computer and internet fraud, mail scam, credit card fraud, bankruptcy fraud, insurance fraud, government fraud, tax evasion, financial fraud, securities fraud, insider trading, bribery, kickbacks, counterfeiting, laundering, embezzlement, as well as economic and copyright/trade secret

theft. From our experience also, while in the main they have been driven by the existence of an environment where power is monopolized over the long-term by only a few social and political elites, it must be understood that greed is the defining character of the crime.

The truth is that we came into full awareness of this pattern of crime in 2002 and went straight to work but dramatically by 2004 it has mutated to a huge sub-regional crisis in West Africa. A lot needs to be said about the social context of the origin and development of this crime: in many of the countries in our region, decades of military autocracy cemented a practice where the networks of criminality hid behind consensual agreements of illegality concealed from the public and shielded by bayonets.

Two months ago in Abuja, at a sub regional police seminar organised by INTERPOL to discuss the challenges of transborder crimes, I had the opportunity to share thoughts with many of our colleagues from the West African sub-region regarding the mutation of aspects of cyberscam when I asked them to understand keenly how a crime replicated itself between 2002 and 2004. Thus in two years a multi-million dollar crime has migrated from the Nigerian geographical space to embrace a wider canvass of the whole sub-region.

The factors which explain this transformation also draw attention to what we must do to overcome the challenge. Two main factors aided this pattern: the free travel protocol which was granted by the ECOWAS treaty; as well as the increasingly developed IT infrastructure in the sub region. These two factors yoked with the poor attitude initially shown towards this fraud because it presumably preyed on foreign victims. These factors originally provided little incentive to do anything about the scammers, whose boiler rooms were growing by the day in other ECOWAS nations that had now become particularly attractive to the scammers such as Togo, Benin, Ghana, Burkina Faso, Senegal, and Cote d'Ivoire among others.

While this criminal practice took root, erstwhile law abiding citizens of host countries, enticed by juicy criminal offers, got recruited into this garish scheme; meanwhile, as our own research pointed out, the Nigerian scammers in exile were moving into a second generation of the criminal practice by acquiring choice properties within the sub region and laundering their tainted money in the world of real estate. They liberating opportunities of cyberworld has ironically fostered a crime pattern that became the main mechanism and predicate reference for a huge money laundering scheme in our region.

Significantly, the half a decade old 'Nigerian cybermail' had, by 2004, acquired a sub-regional character as a 'West African mail', even as Spanish, South African, Australian, British and Canadian 'lottery letters' exploded on the Internet.

Today the patterns are also growing in different dimensions: we now deal more with issues of cloning of websites; falsified representations; internet purchase and other ecommerce kinds of fraud. The criminals notably use fake credit cards unlawfully acquired from websites that provide compromised credit cards as well as from Nigerians legally residing in western countries and who work in the postal systems of such countries. Other typologies we have noticed are through the manufacture of fake cheques, gift cards and other instruments of legal transactions.

Locally the harm is also growing and the domestic economy is groaning. The Nigerian banking industry that hurriedly embraced the credit card system did not carry the law enforcement and criminal justice sector along in the capacity to understand the intricacies and multiple dimensions of the problem. The result is that today we have huge and rising incidence of cybercrime which, sadly are under-reported and for which the law enforcement, prosecutors, and judges are unable to match the crime with appropriate punishment. I speak here of a gap in knowledge which I shall speak more about in a while.

In fully characterizing the practice of cybercrime in Nigeria some issues are fairly settled:

- the perpetrators are youths and thousands of unemployed but highly knowledgeable ones who are computer savvy are involved and they actually drive the process.
- They are well connected through local insider conspiracy in the financial institutions locally as well as with Nigerian immigrant community elements abroad.
- Knowing full well that Nigerian enforcement process has become so vigorous they have migrated to mostly West African and other African nations with weak enforcement mechanisms.

- They also use a mechanism of reshippers mostly in Dubai, the UK, and the West African way stations.
- They enjoy the fact that there are no cybercrime laws in any of these African jurisdictions that they have chose as their relay stations.

The implications for the national economy as well as for international trade are enormous: between 2003 and 2007 we successfully disrupted and blocked transactions worth £300million; €200million; and \$500million respectfully. In the same time span we have successfully prosecuted 97 cybercrime specific offences. As you can imagine the large and broader import is more disturbing. It is leading to the erosion of confidence in genuine Nigerian commercial credibility and today many western countries with France taking the lead have moved to deny Nigerian businessmen and women who are legitimate the rewards of ecommerce. France today requires web camera verification for most online business transactions forom Nigeria.

On our part we continue to shoulder on but we believe the answer relies more in vigorous enforcement strategies. We have excellent working relationship with international enforcement programs that have helped advance these programs. Today we work with the United States Secret Service; the FBI; the SOCA in Britain; the Amsterdam Police, as well as the Australian police.

However there is need for regular engagement with industry to develop strategies that can prevent and curtail these practices. Sad to say that some private sector entities have proved unhelpful. We in particular have failed to enjoy the cooperation of Western Union while on the other hand we have enjoyed the full cooperation of Money Gram. There is also need to enjoy the confidence and cooperation of the level three providers of internet facilities like the Yahoo, Google, and hotmail message carriers. When help had come the result had been wonderful. We successfully shut down 70 websites that provided cloned service for criminality with the assistance of the **IC3** Complaints Center in United States.

I see training and vigorous training as the cornerstone of any worthwhile success in the law enforcement program that will support our effort at attacking cybercrimes in Africa. Our region's capacity to own its own century will depend in large measure on its capacity to promote and maintain a regime of economic security and enhance trade and commercial progress without reference to crime. In this march, effective policing that is in tune with modern democratic culture will be the key. The challenge and focus of training will therefore need to embrace a wing span that stretches from cyber studies, law, criminal justice systems, heavy crime prevention education, international relations, international business practices, forensic science, to the intricate numeric depth of the capital markets jigsaw.

In all these efforts we look forward to collaboration and principled assistance from the international community. I thank you once again for the invitation and I look forward to working with you all.