How Do Real Cybercrime Syndicates Operate?

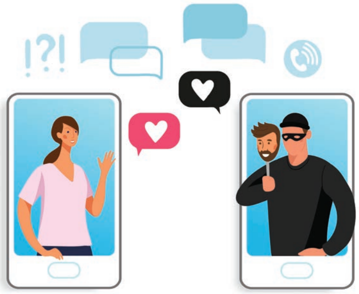
The Case of Online Romance Fraud Syndicates

Francis Kofi Andoh-Baidoo | University of Texas Rio Grande Valley
Martin Otu Offei | Koforidua Technical University
Emmanuel W. Ayaburi | Baylor University and Cleveland State University
Mikko Siponen | University of Alabama

Online romance frauds originating from Africa are typically done by syndicates of 150–200 scammers. We identified three levels: operational level scammers overseen by “chairmen,” who report to the “chairman of chairmen.” Additionally, sympathizers may unintentionally encourage online fraud by their actions or inactions.

Online romance fraud (ORF) is a huge crime business worldwide.[1,2,3,4] ORF involves deceitful online romances to swindle individuals out of their money.[1] The Internet, particularly dating sites, creates a mass opportunity in cyberspace to target victims of cybercrime.[2] In the United States alone, for instance, ORF resulted in a loss of about US$1.14 billion for victims in one year.[5] In addition to financial losses, ORF victims experience various psychological effects (loss of employment, suicidal ideation, and relationship breakdown).[6,7] In the past, ORF offenders approached victims through sending generic messages to several thousands of people, for example, by e-mail or social media. In recent years, more customized approaches are used in dating apps such as Tinder or Momo or online games.

Digital Object Identifier 10.1109/MSEC.2024.3401288
Date of current version: 17 July 2024



©SHUTTERSTOCK.COM/TANYA ANTUSENOK

What Is ORF?

In ORF, after the “dating” between the offender and the victim has started on dating sites, the offender may move the victim to other platforms such as WhatsApp, build trust with the victim, and then ask the victim to send money. Furthermore, ORF offenders have been using information technology (IT) and artificial intelligence (AI) to fake their identities online even before AI became hyped. For example, with the aid of IT, the offender can pose with a gender that satisfies the victim but is different from the offender’s real-life gender. For example, a victim sees an attractive female in a WhatsApp video call, while the person is a male in real life.

Structure of the ORF Gang

Several different ORF gangs operate in a single jurisdiction. In sub-Saharan Africa, an ORF gang is led by a “chairman of chairmen.” Below this position are 10 to 15 chairmen, who report to the “chairman of chairmen.” Typically, one chairman manages 10 to 15 offenders at a time (Figure 1). The “chairmen” are responsible for recruiting and supervising beginner offenders. The offenders form the operational level of the ORF gang and mostly deal directly with the victims.

The literature acknowledges multiple parties’ involvement in ORF operations.[8,9,10] An important group of people that enable ORF is money mules. Most of the transactions that happen in the vicinity of the victims are facilitated by money mules. These individuals allow their banking accounts to be used for money exchange between the victims and the fraudsters. These groups, together with the chairmen, form the middle level of the ORF structure. Money mules are common in crimes involving money. Money mules can collect the money from the banks, or the money is transferred from the victim to the offenders through money mules. Money mules operate in different countries.[8,9]

Sympathizers: Clergy, Musicians, Bank Officials, and Law Enforcement

Some popular persons such as musicians, clergy, and actors could inadvertently embolden online romance fraudsters by their actions or inactions. We call this group sympathizers because by law they are not criminals and may not benefit from the crime, but they wield great power in solving the ORF menace because of the respect accorded to them by society. Some musicians in the African subregion have composed songs that glamorize ORF. Furthermore, sermons of some clergy and failures of some banking officials have motivated offenders to continue to engage in ORF.

Some fraudsters give money to needy persons in society to court acceptance of the society or contribute to community projects (e.g., schools, clinics, and toilet facilities). The offenders also provide community watchdog committee allowances to curb petty stealing within some communities where they live. ORF criminals do these acts to demonstrate good neighborliness and avoid criticisms.

> **They learn about the use of voice recording and voice editing software to make sure their voices and their accents are maintained to continuously deceive their clients.**

Member Recruitment

Traditionally, ORF offenders use public Internet cafés to recruit victims.[10] In recent years, due to improved digitalization, offenders have been using sophisticated technologies to perform ORF.[11] New members are recruited for ORF usually at an Internet café[11] or, more recently, online. The beginner offenders work in groups often between ten and twenty under the supervision of a group leader, the chairman. Offenders openly display their wealth by buying expensive cars and driving in large convoys, which also helps in recruitment as these acts attract others, especially those looking for quick ways to be rich or have no employment. In ORF gangs, the chairman is responsible for the recruitment, training, and supervision of new recruits.

During training, the recruits are emboldened and equipped with tools and skills to create multiple accounts on different dating sites with attractive varied profiles (mostly fake) to lure prospective victims to start chatting online in the name of love. The chairmen teach the recruits to familiarize themselves with used templates, key words, and love expressions and how to use these words and phrases to keep an online romance conversation going. The recruits also learn about the use of AI-enabled image editing tools to change images that reflect their line of conversation to sustain the interest of the victims over a long period of time. They learn about the use of voice recording and voice editing software to make sure their voices and their accents are maintained to continuously deceive their clients. Under the chairmen, the recruits gradually learn about tactics and tricks to master over time.

The Rules of the ORF Gang

There are individual offenders who do ORF solo. However, loyalty is

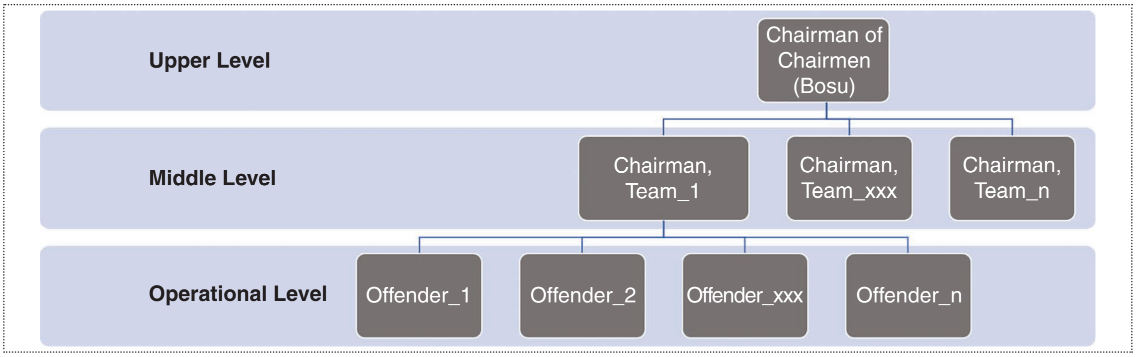


Figure 1. The ORF syndicate structure.

required from those who are members of the syndicate. Each offender can deal with as many clients as they can manage. When a beginner fraudster is not careful and allows the gang to lose a valuable client, that offender is reprimanded by the chairman. The punishment can start from a stern warning and escalate to expulsion from the gang and losing all privileges such as protection from law enforcement, feeding, friendship, and accommodation. When the beginner offender is not bringing money as expected, they are encouraged to do more or be shown the exit. For some offenders, ORF is their full-time job.[9,12]

This has resulted in ORF scammers in Africa shifting to online payment systems, where it is easy for offenders to receive money from victims without being questioned about the money.

Cooperation Within the Gang

Figure 2 depicts the coordinated operational process of the ORF syndicates and the tools involved. The thinking that cybercrimes is a process or occurs in stages is essential in understanding the operationalization and the development of mitigating strategies.[13,14] When a beginner or operational-level offender faces challenges in persuading a potential victim to send money, they may ask help from the "chairman." The chairman then continues the conversation with the victim and brings his (the individuals are mostly males) experience to bear on the victim. In such cases, the proceeds of such exploits are shared in an agreed ratio among the offenders and the "chairman." In turn, when the chairmen hit a sledge, they grant access to their chats with their clients to the "chairman of chairmen," who will continue with the romantic conversation with their in-depth experience to convince the victim to send more money.

Sharing of Proceeds and Money Laundering

The proportion of the proceeds that an offender receives from a successful operation with a victim is determined by the "chairman of chairmen" and the amount of people involved. The highest proportion goes to the most senior person. Offshore accounts are sometimes opened for offenders by bank managers who may or may not be privy to the source of the funds.

Preventing Cybercrime Requires a Deeper Understanding of the Crime Settings

New thinking is needed to prevent cybercrimes. For example, arresting local money mules in Western countries, while needed, is not effective in preventing the occurrence of crime. Similarly, banks and money transferring organizations have increased security checks. This has resulted in ORF scammers in Africa shifting to online payment systems, where it is easy for offenders to receive money from victims without being questioned about the money.

Although most citizens in ORF-prevalent regions oppose the crime, their influence is weaker than that of those promoting ORF as a career during economic downturns. Preventing ORF requires fundamental understanding of the crime and local settings and requires international cooperation among all stakeholders including law enforcement agencies, educational institutions, and people in governmental and nongovernmental institutions. Those in authority or with societal influence must speak against the ORF crime and publicly state the role that each player in the syndicate

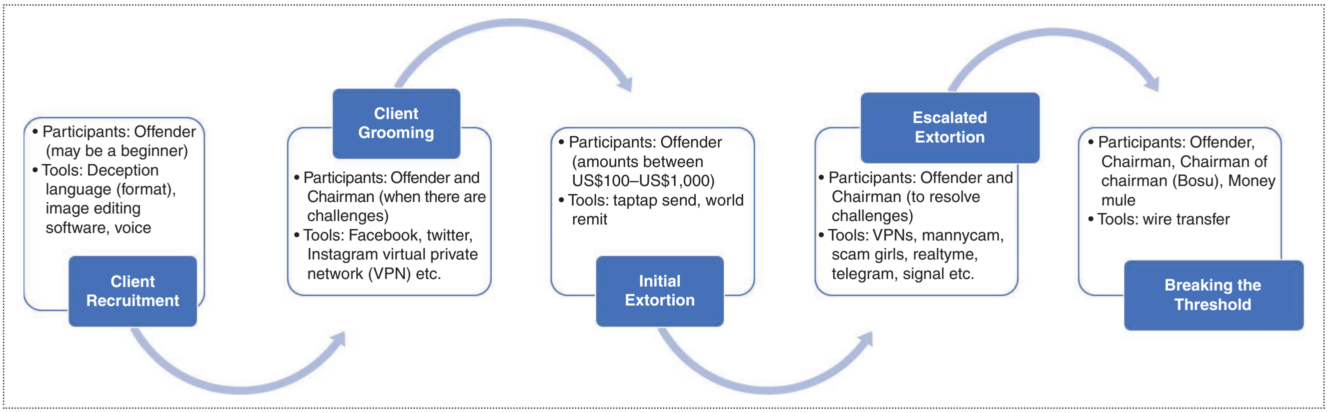

• Participants: Offender (may be a beginner)
• Tools: Deception language (format), image editing software, voice
Client Recruitment
Client Grooming
• Participants: Offender and Chairman (when there are challenges)
• Tools: Facebook, twitter, Instagram virtual private network (VPN) etc.
• Participants: Offender (amounts between US$100–US$1,000)
• Tools: taptap send, world remit
Initial Extortion
Escalated Extortion
• Participants: Offender and Chairman (to resolve challenges)
• Tools: VPNs, mannycam, scam girls, realtyme, telegram, signal etc.
• Participants: Offender, Chairman, Chairman of chairman (Bosu), Money mule
• Tools: wire transfer
Breaking the Threshold

Figure 2. The ORF process.

and other sympathizers are contributing to the crime to persuade the youth to eschew ORF. Governments and for-profit and nonprofit organizations, while aiming to provide jobs for the youth to minimize the enticement that ORF presents to the youth, should emphasize how ORF is not a long-term job solution. Educational institutions should develop programs and market the potential of gainful employment for individuals with IT skills where people with tendencies to be indulged in ORF will be trained. The local universities' IT skills training effort should be in collaboration with industry to create internships and job offers for these students to minimize ORF criminals. Banks need to implement measures to close loopholes that enable money laundering from ORF operations in affected economies. Furthermore, online service providers including dating platforms are encouraged to protect their users,[15] and this may include increased efforts to detect syndicates on these platforms that should be reported to international law enforcement agencies such as INTERPOL. The societies in the sub-Saharan Africa region must refuse to celebrate the grandiosity of wealth gained from ORF crimes with public institutions refusing permits for philanthropic acts known to be the results of ORF crimes. Law enforcement agents should be empowered and equipped with technical knowledge and physical tools and skills to prosecute people involved in ORF crimes. It is the duty of the legal authorities to find ways to develop mechanisms by which first offenders are given the opportunity to reintegrate with society but repeat offenders are punished to deter other potential criminals.

Since developed nations suffer the damages of ORF the most, it is incumbent on these nations to provide incentives to developing nations who use foreign aid from developed nations to support programs that prepare the youth and develop programs to reduce unemployment among the youth. Nonprofit organizations should also be motivated to support programs that provide economic benefits for unprivileged and economically challenged youth to receive financial support in their educational pursuits. ■

Acknowledgment

The corresponding author is Mikko Siponen.

References

1. M. Offei, F. K. Andoh-Baidoo, E. Ayaburi, and D. Asamoah, "How do individuals justify and rationalize their criminal behaviors in online romance fraud?" *Inf. Syst. Frontiers*, vol. 24, no. 2, pp. 1–17, 2020, doi: 10.1007/s10796-020-10051-2.
2. M. F. Vilardo, "Online impersonation in securities scams," *IEEE Secur. Privacy*, vol. 2, no. 3, pp. 82–85, May/Jun. 2004, doi: 10.1109/MSP.2004.19.
3. E. Fletcher. "Romance scammers' favorite lies exposed." Federal Trades Commission. Accessed: Feb. 9, 2023. [Online]. Available: https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed
4. R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*. Hoboken, NJ, USA: Wiley, 2020.
5. L. Fair. "'Love Stinks'—When a scammer is involved." Federal Trade Commission. Accessed: Feb. 13, 2024. [Online]. Available: https://www.ftc.gov/business-guidance/blog/2024/02/love-stinks-when-scammer-involved
6. C. Cross, M. Dragiewicz, and K. Richards, "Understanding romance fraud: Insights from domestic violence research," *Brit. J. Criminol.*, vol. 58, no. 6, pp. 1303–1322, Oct. 2018, doi: 10.1093/bjc/azy005.
7. M. T. Whitty, "Is there a scam for everyone? Psychologically profiling cyberscam victims," *Eur. J. Criminal Policy Res.*, vol. 26, no. 3, pp. 399–409, 2020.
8. P. E. Adejoh, "Feeling of safety among residents in metropolitan Lagos, Nigeria," *IFE PsychologIA, Int. J.*, vol. 31, no. 1, pp. 133–145, Mar. 2023. [Online]. Available: https://hdl.handle.net/10520/ejc-ifepsyc_v31_n1_a14
9. A. E. Jegede, "Cyber fraud, global trade and youth crime burden: Nigerian experience," *Afro Asian J. Social Sci.*, vol. 4, no. 5, pp. 2229–5313, 2014.
10. O. Tade and I. Aliyu, "Social organization of internet fraud among university undergraduates in Nigeria," *Int. J. Cyber Criminol.*, vol. 5, no. 2, pp. 860–875, Dec. 2011.
11. A. C. Tambe Ebot, M. Siponen, and V. Topalli, "Towards a cybercontextual transmission model for online scamming," *Eur. J. Inf. Syst.*, pp. 1–26, May 2023, doi: 10.1080/0960085X.2023.2210772.
12. S. Lazarus, "Birds of a feather flock together: The Nigerian cyber fraudsters (Yahoo Boys) and hip hop artists," *Criminol. Criminal Justice Soc.*, vol. 19, no. 2, pp. 63–80, 2018.
13. M. T. Whitty, "Mass-marketing fraud: A growing concern," *IEEE Secur. Privacy*, vol. 13, no. 4, pp. 84–87, Jul./Aug. 2015, doi: 10.1109/MSP.2015.85.
14. D. Maimon and E. R. Louderback, "Cyber-dependent crimes: An interdisciplinary review," *Annu. Rev. Criminol.*, vol. 2, no. 1, pp. 191–216, Jan. 2019, doi: 10.1146/annurev-criminol-032317-092057.
15. B. Edelman, "Least-cost avoiders in online fraud and abuse," *IEEE Secur. Privacy*, vol. 8, no. 4, pp. 78–81, Jul. 2010, doi: 10.1109/MSP.2010.132.

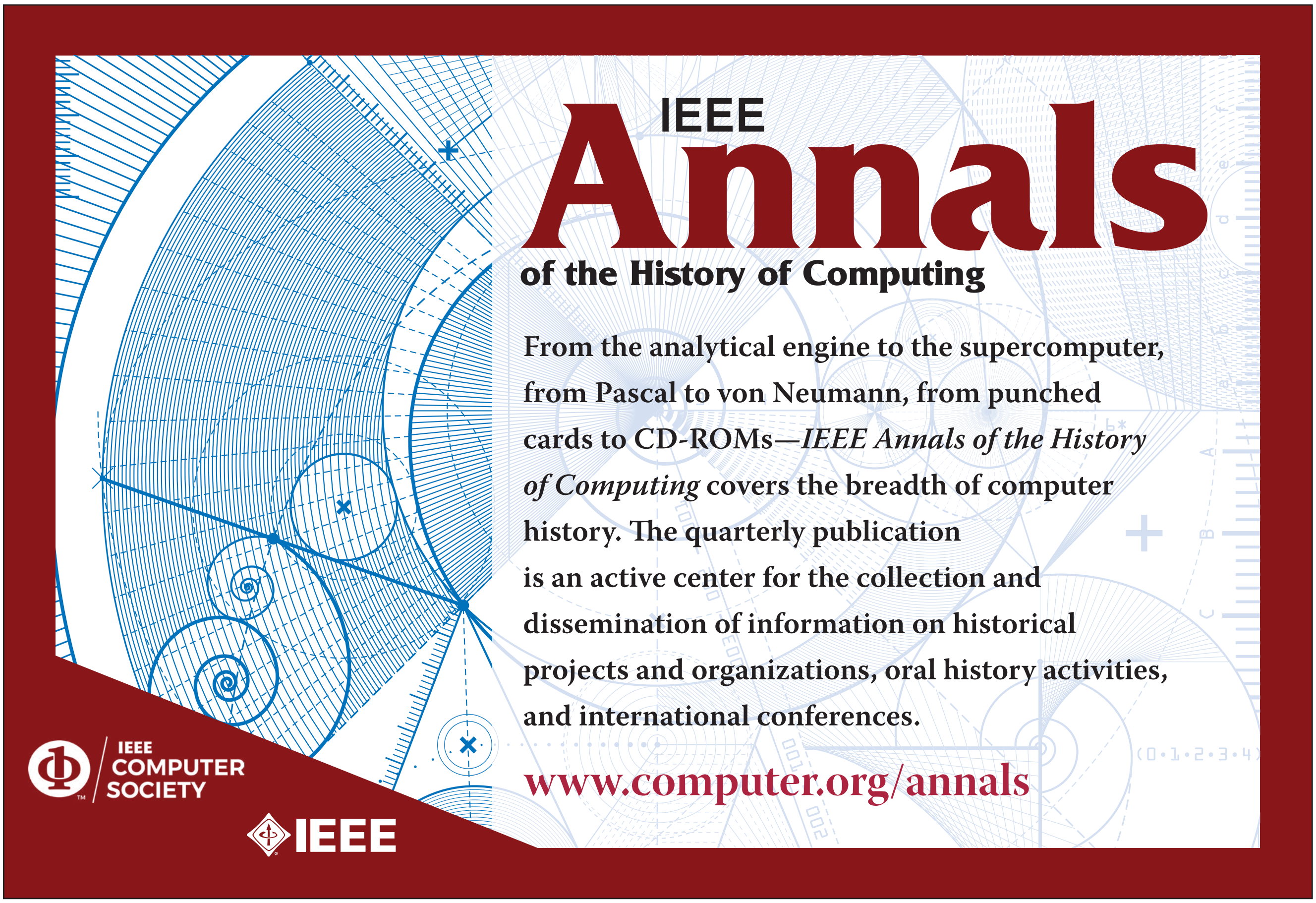
Francis Kofi Andoh-Baidoo is a professor at the Department of

Information Systems, Robert C. Vackar College of Business and Entrepreneurship, University of Texas Rio Grande Valley, Edinburg, TX 78359 USA. His research interests include business analytics, information and communication technology for development, and information security and privacy. Andoh-Baidoo received a Ph.D. in information systems from Virginia Commonwealth University. Contact him at francis.andohbaidoo@utrgv.edu.

Martin Otu Offei is a senior lecturer in computer science at Koforidua Technical University, EN-112-3991, Korforidua, Ghana. His research interests include management information systems, IT in businesses and cybercrimes, and Internet fraud-related crimes. Offei received a Ph.D. in management information systems from Kwame Nkrumah University of Science and Technology. Contact him at martin.offei@ktu.edu.gh.

Emmanuel W. Ayaburi is an incoming assistant professor of information systems at Baylor University, Waco, TX 76706 USA. He was a faculty member of Cleveland State University, Cleveland, OH 44115, USA. His research interests include behavioral information systems security and privacy, economics of information systems, and knowledge sharing. Ayaburi received a Ph.D. in information systems from the University of Texas at San Antonio. Contact him at yanbed@gmail.com.

Mikko Siponen is a professor of information systems at the University of Alabama, Tuscaloosa, AL 35487 USA. His research interests include cybersecurity management, information systems security, cybercrime, and IT ethics. Siponen received a Ph.D. in philosophy and a Ph.D. in information systems from University of Joensuu. He is an invited member of the Finnish Academy of Science and Letters. Contact him at tmsiponen@ua.edu.



Digital Object Identifier 10.1109/MSEC.2024.3425123