

DISCOURSE DYNAMICS OF BANK FRAUD ALERTS IN NIGERIA
Faith Ekata AMUZIE, Chukwuma Daniel EZIRIM & Jennifer Osayi AGHO
Department of English Studies, Benson Idahosa University

Abstract

This study examined the discourse practices of online fraud alerts issued by Nigerian banks to warn customers against fraudulent activities. In the dynamic landscape of financial transactions, the discourse of fraud alerts is pivotal in cautioning clients, mitigating risks, and safeguarding the banking sector's integrity. The research analysed 22 digital bank fraud alert posters, sourced from customers' emails, official social media platforms, and notification channels, with the aim of uncovering the strategies employed by financial institutions to warn, engage, reassure, and communicate effectively with their customers. The study was guided by Genre Theory, which provides a framework for understanding how forms of communication are structured, the conventions they follow, and the expectations they create in specific contexts. Its application to bank fraud alerts facilitated an exploration of their linguistic features, communicative purposes, and broader significance in financial communication. Findings indicate the prevalence of particular alert types and discourse strategies, reflecting banks' efforts to build awareness, protect clients, and enhance fraud prevention. The study contributes insights into how financial institutions deploy language to foster trust and resilience in an era of digital banking, with relevance for clients, banks, and fraud prevention agencies alike.

Keywords: Bank, Fraud alert, Discourse, Nigeria, Genre Theory.

Introduction:

The discourse of bank fraud alerts revolves around a complex issue with significant implications for businesses, individuals and society. Fraud, a universal phenomenon (Nwanaka, 2022), is an illegal, intentional, dishonest act by a person or group to deceive others for selfish gain, causing financial damage to the victim and benefiting the perpetrator (Hao Sun et al., 2023; Badejo et al., 2017; Nwanaka, 2022). Fraud also occurs in different types with diverse causes for its occurrence (Olatunji & Adekola, 2014; Harte & McHone, 2019). With the ever-evolving landscape of online banking and its security issues, financial institutions frequently invest in security measures (Owolabi, 2010; Rahman, 2021; Buckley et al., 2016). These measures help customers navigate the complexities of securing their financial transactions and accounts, protect them against potential fraud, and enable financial institutions to build a more resilient and secure online banking environment. Bank fraud alerts are one such key strategy deployed by financial institutions to

protect their clients against potential fraud. These alerts vary from warning alerts, informative and reassuring alerts, call-to-action alerts, notification alerts, to educational alerts; and they may be delivered through SMS, in-app notifications, email notifications, online banking alerts, and social media alerts. These online alert types are key elements that allow banks to communicate with their clients regarding potential fraud.

The emergence of online banking alerts is attributed to several factors. One key factor is the digitisation of financial services and the recognition by financial institutions of the need for timely and efficient communication with their customers to enhance the security and convenience of their digital platforms, particularly as online banking gained popularity in the early 2000s (Pousttchi & Dehnert, 2005; Buckley et al., 2016). The outcome of this recognition is the development of automated alert systems to notify customers about various activities. Another such factor is the increasing prevalence of cyber fraud and identity theft, which have led financial institutions to understand the importance of

empowering their customers with real-time notifications to assist them in monitoring and protecting their accounts from fraudulent activities (Zelege & Assefa 2020). In addition to these is the rising necessity for customers to have secure and convenient digital banking experiences, coupled with ongoing efforts by banks to combat fraud and enhance customer trust (Karjalainen et al, 2002), advent of e-payment platforms. As a result, online banking alerts have become a crucial tool in the fight against financial crime, thus providing customers with an additional layer of security and control over their financial transactions. Today, these alerts have become an integral part of the online banking experience, offering customers peace of mind and the ability to stay informed about their financial transactions at all times. The current study investigates the discourse dynamics of digital bank fraud alerts in Nigeria to understand how banks in Nigeria engage and effectively communicate with their customers regarding potential fraud. The objectives of this study included identifying the communicative strategies, lexis and structure used in online bank fraud alerts.

Relevant studies

Fraud is not a recent phenomenon. Considerable research on various aspects of fraud exists (Harte & McHone, 2019; Rahman, 2021; Olaoye & Adekola, 2014; Badejo et al, 2017; Breeze, 2012; Gillen, 2016). However, one significant area of interest in this study is fraud-related discourse. Scholars such as Carter (2023), Olajimbiti (2018), Furnell and Emm (2008) and Blommaert (2005) conducted studies around persuasive discourse in relation to fraud. Carter (2023) investigated 'fraudulence', the language of fraudsters, focusing on how fraudsters successfully deceive victims into submission in telephone-mediated fraud without the victim recognising the context as harmful. The study indicates that fraudsters deploy social and interactional expectations and manipulative power relations to lead victims into a false reality. In another study, Olajimbiti (2018) examined email fraud spam, and the study indicates that cyber fraudsters use business and religious contexts, familiar patterns and strategic persuasive language resources to defraud potential victims. In a related

study, Blommaert (2005) examined scam emails and revealed that scammers construct manipulative rhetoric that mimics credible sources by crafting authority and legitimacy through cultural references and linguistic borrowings from official communications. Furnell and Emm (2008) explored phishing emails and identified that these emails deploy urgency, impersonation, grammatical inconsistencies and recurrent structural and linguistic patterns to manipulate recipients.

In a different but relevant study on discourse and fraud detection, Suna et al (2023) investigated textual risk disclosures in the annual financial reports of some organisations. They discovered that the parts of speech used in textual risk disclosures of annual financial reports can provide significant ability for detecting financial fraud, thereby improving the performance of financial fraud detection. In another loosely connected study, Osisanwo & Olaniyi (2021) considered the discourse representation of fraudsters in Nigerian newspapers. They concluded that Nigerian papers frame fraudsters as moneybags, youths, students, fetishists, impersonators and drug peddlers through the textual elements of identifying, stating, narrating and indicting on the one hand, and the visual strategies of individualisation, collectivisation, location and colouration on the other.

Although scholars like Ayeni (2020), Balfageeh (2016), and Gunnarsson (2000) completely took a detour from the above studies, their investigations on banking discourse are very relevant to the current study. Ayeni's (2020) study reveals that bank service providers adopt inclusion, directness, informality, and face-saving strategies to gain new customers and retain old ones. Balfageeh (2016) observes that banks leverage personalisation, intertextuality, and interdiscursivity, and often appeal to patriotism and religious sentiments to redefine their relationship with society, while the findings from Gunnarsson (2000) reveal that bank discourse is significantly influenced by organisational culture as management ideas tend to shape communication patterns and national cultural differences reflected in disseminated images.

Certainly, these studies provide perspectives and contribute to a robust discourse on fraud, and also underlie the need for discourse-based studies on fraud, particularly in a developing country like Nigeria. With the current focus on bank fraud alerts, which are underexplored as a distinct genre within institutional discourse, this study would inform best practices for crafting clear, timely and persuasive fraud notifications. The study will also contribute to financial literacy, customer security, and trust in the banking sector, as well as inform strategies for law enforcement, enhance cybersecurity measures, improve public awareness and support anti-fraud policy development.

Method and data

This study explored the discourse of bank fraud alerts, focusing on their types, rhetorical moves, discursive strategies, syntactic structures and lexical choices. Twenty-two (22) digital fraud alert posters from four financial institutions, namely UBA, First, Zenith and Access banks, were collected from customers' emails, social media handles and notifications as data. These were analysed to identify patterns and strategies employed to achieve effective communication and to convey warnings and instructions. The study draws on Genre Theory to understand how fraud alerts are structured and function as an advisory genre within the banking sector. Although numerous definitions of genre exist (Miller 1984,

Amy Devitt 1993, John Swales 1990), this paper adopts the position that Genre Theory views diverse communication types as entities that are deliberately structured and function within specific contexts. Bank fraud alerts are situated within the broader context of institutional discourse, where banks aim to mitigate risk and influence customer behaviour through concise and persuasive communication.





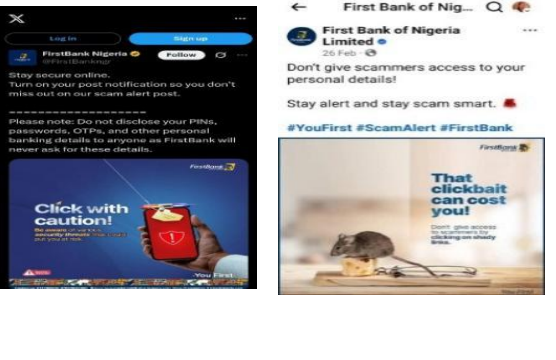

The unique characteristics and linguistic elements of bank fraud alerts are shaped by their communicative purposes within the broader context of financial communication. The analysis of bank fraud alerts using this theory would therefore provide insights into the specific communicative strategies and linguistic features that shape fraud alerts and make them unique as a generic entity, engendering an understanding of the conventions and expectations associated with this form of communication, including the language used, the typical structure, and the intended audience response.

4. Findings/discussion

The results section clearly identifies the main findings, including the types of alerts and the linguistic strategies employed. The analysis examines how language features are strategically deployed to warn bank customers of potential fraud and convey precaution.

4.1 Data presentation

Table 1: Data Samples

 <p>UBA Fighting Fraud Together! Fraud Awareness Week 2023</p> <p>JUST HANG UP Ignore calls asking you to send the 16-digit number on your credit card, the expiration date, CVV and card name to help you protect your debit card information. UBA will never ask for this information.</p> <p>IT'S A SCAM DON'T FALL FOR IT Report all suspicious fraudulent activities to our Fraud Alert line on 01 2808 800 or email fraudhelp@uba.com.ng</p> <p>We're excited to start the Fraud Awareness Week 2023, a dedicated initiative aimed at raising awareness and preventing financial fraud.</p> <p>Take a second pause from your phone when you receive calls, PIN, OTP or SMS with requests. Together, we can conquer fraud.</p>	 <p>UBA Be a step ahead of scammers</p> <p>Protect your money from fraudsters with 3 simple money saving tips:</p> <ul style="list-style-type: none"> Secure your account - Pin protect by pinning or locking your app. Don't let your account details - Protect the CVV of your debit card - and remember that you can't change it. Keep it private - Do not give your PIN, account number, PIN, CVV, OTP, password, information or account details with anyone. <p>If you think you have been a victim of fraud, please report it to our Fraud Alert line on 01 2808 800 or email fraudhelp@uba.com.ng</p>
 <p>Zenith Bank ... Follow</p> <p>SCAM ALERT! Please note that #ZenithBank will never call, SMS or email you requesting for your personal banking information.</p> <p>Also please be informed that #ZenithBank does NOT have a WhatsApp number and will never request for your sensitive information via the any platform.</p> <p>SAFEGUARD YOUR ACCOUNT Zenith Bank never NEVER call, SMS or email you requesting for your personal banking information. Please note that #ZenithBank does NOT have a WhatsApp number and will never request for your sensitive information via the any platform.</p> <p>Reconfirm Credit Alerts Before You Release Goods #StaySafe</p> <p>256 likes zenithbankplc A new scam by fraudsters involves sending fake credit alerts to unsuspecting store owners in a bid to get them to release goods. Please reconfirm credit alerts from walk in customers using any of our digital channels before parting with goods.</p>	 <p>Zenith Bank Plc Internet banking login details or other account-related information.</p> <p>#StaySafe #CurbTheSpread #Security #ZenithBank</p> <p>COVID-19 SCAM ALERT NOTICE</p> <p>We have advised that some fraudsters are claiming to be employees of various banks and asking fraudulent phone calls to provide requesting for details of their bank debit cards and ATM PINs, to facilitate the disbursement of a purported COVID-19 relief package from the Federal Government.</p> <p>Please be advised that this is a scam being perpetrated by fraudsters to access your bank details. Do not provide any account information (including account number, PIN, CVV or banking details) and do not provide any information about your bank details, debit card and ATM PIN.</p> <p>Thank you.</p>
 <p>First Bank of Nigeria 26 Feb</p> <p>Don't give scammers access to your personal details! Stay alert and stay scam smart.</p> <p>#YouFirst #ScamAlert #FirstBank</p> <p>Click with caution! Do not click on links from unknown sources. Do not click on links from unknown sources. Do not click on links from unknown sources.</p> <p>That clickbait can cost you! Don't give access to your account to anyone who is asking for money.</p>	 <p>#FirstBankCares #EnablingYou</p> <p>Be Scam Smart</p> <p>Scammers are getting smarter. Do not give access to your account to anyone who is asking for money.</p> <p>Fraudsters are always on the lookout for their next victim. Don't let it be you.</p> <p>Keep your records with us up to date at any of our branches</p> <p>Think twice before you click. Protect your money from fraudsters.</p>



Source: Current research

Table 1 comprises 16 data samples used for the study. There are four rows, each containing 4 different messages from four banks. The first row contains fraud messages from UBA, while the second, third and fourth rows contain messages from Zenith, First and Access banks, respectively. These are representative data samples from the downloaded digital fraud posters used for the study.

Table 2: Bank fraud alert types

Alert types	Text samples
Warning alerts	"Think twice before you click"
Information and reassuring alerts	"The merger between Access Bank and Diamond Bank will never require you to disclose any personal account details. If you have divulged such information already, or have lost your card or phone, please call 01-2712005 immediately."
Call to action alerts	Make it difficult for scammers to rip you off
Notification alerts	Ignore calls asking you to send the 16-digit number on your credit card, the expiration date, CVV and card name to help you protect your debit card information. UBA will never ask for this information. IT'S A SCAM, DON'T FALL FOR IT.
Educational alerts	12 scams of Christmas, 'tis the season for holiday scams, beware of these scams: (1) New currency scams (2) fraudulent text messages (2) POS scams (4) Look-alike websites (5) Phishy emails (6) Debit card fraud (7) Fake job postings (8) Delivery scams (9) Free gifts cards fraud (10) Malicious holiday e-cards (11) Online shopping scams (12) Christmas loan scams
Security alert	Be scam smart. Fraudsters are always on the lookout for their next victim; don't let it be you.
Ongoing activity alert	Dear Mary....There was a successful login to your ...mobile account....kindly see login details below...if you did not login to your...mobile account, kindly contact

Source: Current research

Table 2 presents text samples that indicate the types of fraud alerts discovered in the data. There were seven (7) types of fraud alert comprising warning, information and reassuring, call to action, notification, educational, security and on-going activity alerts. These are further discussed in the body of the work.

4.2 Sample analyses of discursive and linguistic strategies

The section presents samples of text analyses derived from the data. The analyses are based on the linguistic, rhetorical moves, and discursive features identified in the texts. The analyses are classified according to specific features and each comprises examples and one representative analysis.

4.2.1 Directness, clarity and conciseness of language

The data reflects directness, simplicity, clarity and conciseness in language as the alerts are void of ambiguity and superfluity. For example, the following samples indicate this style of language use: the simple sentence “Together, we can conquer fraud”; the NP “Fraud Awareness Week 2023”; the participial NP “Fighting fraud together”; the simple interrogative sentence “Suspect anything fishy?”; the simple imperative sentence, “Stop, don’t click or share” and the compound sentence, “Take a stand against fraud: never share your card details, PIN, OTP or BVN”. A sample analysis is presented below:

Text 1

“Take a stand against fraud: never share your card details, PIN, OTP or BVN”

This text sample suits a bank fraud alert genre type. Like the other examples listed above, its core purpose is to educate and warn customers about protecting their financial information, and this aligns with the function of bank fraud alerts. The text represents an institutional and security advisory alert message aimed at warning, educating and instructing bank clients on the prevention of financial fraud by avoiding risky behaviour. It is a two-move structure that begins with move-1 as a call to action and appeal (“Take a stand against fraud”) to the client in order to engage the customer’s agency and moral responsibility. The move 2 acts as an instruction and warning (“Never share your card details, PIN, OTP or BVN”), thus acting as a direct prescriptive

action guidance. The imperatives, “Take a stand...” and “Never share...” while creating a commanding and urgent tone, the “Never share” part highlights a negative directive that emphasises prohibition, a common element in safety-critical genres

In addition, the list “card details, PIN, OTP or BVN” is a paratactic list that reinforces clarity and salience. The words are listed one after the other without connectives like ‘or’, ‘but’, ‘and’ or any other subordinating elements. This style is often used for clarity, brevity and emphasis. This use also exhibits a telegraphic style where unnecessary words are omitted and there are no hedging or explanations, thus reflecting the constraints of notification genres and the urgency of the message. The telegraphic style is always concise and direct, and omits unnecessary words. It is characterised by brevity and economy of words, so there are no articles (or very limited use), prepositions and other non-essential words and directness by a clear and straightforward message, conveying a clear message efficiently. In all, these ensure that recipients quickly grasp the nature of the alert and that the wording does not confuse the recipient, and of course, prompt immediate action, if need be. The discursive positioning of the text is such that it positions the bank as a guardian of customer security while also placing responsibility on the customer to take preventive action. This pattern reflects moves and strategies typical of brief warning notices in financial institutions. This result aligns with the finding by Ayeni (2020) that directness is a language strategy banks utilise for customer engagement.

4.2.2 Strategic use of specific institutional details

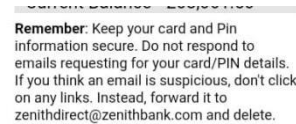
These fraud alert messages reflect a strategic use of specific details that enhance the effectiveness of banks’ communication. These details may include the name of the bank, logo, phone numbers, official email accounts, registered addresses, social media handles, and contact

information. For example, the samples below

indicate the use of such details:



“Report suspicious calls to 07080625000, 014485500 or email abuse@firstbanknigeria.com”



The strategic use of institutional details helps to establish credibility and trust, and also enables the recipient to identify the source, authenticity and legitimacy of the communication. For instance, the name and logo of the UBA and Zenith Banks are prominently displayed to signal authenticity. These familiar elements can allow customers to distinguish real messages from phishing ones. This strategy helps the bank create a brand identity and trust that reinforces the bank's legitimacy and reduces confusion and scepticism on the client's side. Further, the data also reflects the use of official domain names such as www.zenithbank.com, abuse@firstbanknigeria.com and cfc@ubagroup.com etc., thus allowing banks to be consistent in their official channels, avoid generic addresses and ensure coherence with other communications from the banks. The alerts also include verifiable and support phone numbers that encourage user action through confirmed and secure channels in order to reduce the chance of bank customers engaging with fraudsters. Additionally, the alerts contain specific security disclaimer information of banks (“Zenith Bank will never call, SMS or email you to request your card details...”; “Access Bank will never send you a link to an external website or ask for your log in details...”) that provide a legal layer of formality and transparency to the message. These details function in dual capacity to first help banks fulfil regulatory requirements and establish these messages as part of official banking correspondence; and secondly, they help recipients to verify the authenticity of bank alert messages.

4.2.3 Actionable language use

Another common feature of these bank alerts is the strategic use of actionable language. Actionable language acts as a prompt to the reader to take specific actions. For example, these language samples highlight this phenomenon:

“kindly contact...”; “...send an email to...”; “....don't click on any link....”; “...instead forward it to...”; “...never share your card details...”; “...call our fraud help desk....”; “...stop! don't click or share...”; “...call us on...”; “....Make it difficult for scammers to rip you off....”; “Protect your money by...”; “...Keep it private...”; “.....Don't let your guard down...” etc.

These structures act as instructions and imperatives for customers to act in certain ways. The messages aim to educate and empower customers to protect themselves from financial scams and fraud by doing certain things or taking certain actions. “*Kindly contact*” is a polite request for communication, “*Send an email to*” is a specific action for reaching out, “*Don't click on any link*” is a warning against potential phishing or malware, “*...Instead forward it to*” is an alternative action for handling suspicious messages. Further, phrases like “*never share your card details*” and “*don't click or share*” are security warnings that instruct customers on what not to engage in and they aim to protect customers from phishing and scams. Instructions like “call our fraud help desk” and “call us on” provide customers with clear actionable steps to take, while messages like “Protect your money by...” and “Keep it private” act as protective measures and emphasise the

importance of safeguarding financial information. *"Don't let your guard down"* and *"Make it difficult for scammers"* encourage customers to remain cautious and be vigilant.

These language resources are part of banks' security advisory and communication protocol for safety guidelines against fraud. They indicate banks' efforts to educate and empower customers to protect themselves from financial scams and fraud, thus acting as instructions and imperatives for customers to act in a certain manner.

4.2.4 Language of institutional safeguards and security measures:

The alerts equally highlight the use of language indicating security measures. These are institution-based and are often formal, cautious and action-oriented in tone. For example, we have:

"Suspect anything fishy? Call our fraud help desk..."; "Suspect anything fraudulent? Please contact our Fraud Help Desk on.....or email us on....". and "Report all suspicious fraudulent activities to....." "... will never ask for ..."

These linguistic resources enable banks to encourage vigilance, prompt immediate actions, communicate responsibility and caution, and provide institutional assurance and responsibility, thus showing their proactive role in security. Some of these language uses are action-oriented instructions that act as direct guidance for taking action (Call our fraud helpdesk), encourage suspicion and alertness (Suspect anything fraudulent?), and reinforce institutional assurance and safe communication practices (...will never ask for...). The language not only directs or redirects customers to channels in case of suspected fraud, but it also helps signal how banks handle security matters and communication, what customers should expect of the banks and the type of behaviour customers need to avoid risk, thus building trust and reassuring customers of the secure practices of banks.

4.2.5 Educational language use

Some alerts contain educational components, providing information on common fraud schemes, scammers' activities and tips to avoid falling victim to scams. Examples include

"Scams come in different forms", "Here are a few ways to protect yourself", "12 scams of Christmas...", "They pretend to be our representative and ask for sensitive information to help solve your problems", "They lurk in the comment sections of social media pages, trying to scam you with fake accounts that look convincing" etc. The text below is analysed for further understanding:

12 scams of Christmas, 'tis the season for holiday scams, beware of these scams: (1) New currency scams (2) fraudulent text messages (2) POS scams (4) Look-alike websites (5) Phishy emails (6) Debit card fraud (7) Fake job postings (8) Delivery scams (9) Free gifts cards fraud (10) Malicious holiday e-cards (11) Online shopping scams (12) Christmas loan scams

This text has a communicative intent to educate customers about fraud patterns, warn customers and promote vigilance. It is advisory and highlights common scams that may occur during the Christmas season. The text has an attention-grabbing title ("12 Scams of Christmas"), obviously borrowed from the cultural reference, "12 Days of Christmas". It provides a clear warning: "Beware of these scams" and specific examples by listing 12 types of scams, thus providing awareness and education. The purpose is therefore to educate customers on potential holiday scams and empower them to protect themselves and their finances. It is a fraud-prevention advisory alert. Somehow, this finding highlights the scholarly positions that fraudsters deploy manipulative rhetoric as reflected in these bank educational rhetoric ("They pretend to be our representative and ask for sensitive information to help solve your problems", "They lurk in the comment sections of social media pages, trying to scam you with fake accounts that look convincing") that appear as credible sources, familiar contexts like business, strategic persuasive language resources and impersonation to defraud potential victims (Carter, 2023; Olajimbiti, 2018; Furnell and Emm, 2008; Blommaert, 2005).

4.2.6 New media discourse features

The data contains new media discourse features, one of which is the convergence of texts, images, symbols, signs, and pictures with sharp and attractive colours in one place. For instance, the image below is a classic example:

Fig. 1



In this fraud-related bank notification, this image brings together texts and images, and serves the preventive and cautionary functions of visually warning customers to be vigilant about their card security and cautioning them about the risks of card theft or misuse at point-of-sale machines (ATMS). This image shows a masked figure in black, representing a fraudster or engaging in unauthorised or illegal financial activity, specifically card theft or misuse.

The large red prohibition symbol (the circle with a slash) is a universal signal of “Do not” or “Prohibited,” indicating that the depicted fraudulent behaviour is unacceptable and illegal. The credit card in his hand represents a stolen or misused item, reinforcing that the fraud is card-related, while the ATM and POS machines in the background are common points of vulnerability where card fraud can occur through skimming,

cloning or unauthorised transactions. Pairing the image with the compound word “Fraudalert” reinforces the idea of warning against fraud, creating a powerful, high-impact warning. The image thus works as a visual shorthand for danger and illegality, and immediately signals risk, making it effective language for quick scanning. The compound word “Fraudalert” functions as a headline-style warning, calling for attention in an urgent tone and acting as a genre marker in bank communication.

Another addition to this is the use of #tags, a discourse pattern in new media. Examples include #ZenithBank, #YouFirst, #ScamAlert, #FirstBank etc. These #tags function as digital metadiscourse tools used to frame alert messages, assert authorship and enhance customer engagement in addition to reinforcing the protective role of the bank. #YouFirst appears to be a bank’s slogan; it helps reinforce the brand and identity of the bank. #ZenithBank helps with source verification, helping clients to distinguish between real and fake alerts and at the same time adding a layer of authenticity and credibility. These #tags also aid visibility and online searches, and thematic categorisation of content into topics and themes (#Fraudalert) – once a customer sees this, he/she automatically knows what the alert is about. In addition to the convergence of media elements and #tags, these alerts also comprise symbolic images. For example, the cropped images below are from the data:

Table 3: Fraud alert images

	<p>Fig 2</p>	<p>Fig 4</p>
<p>Fig 3</p>		<p>Fig 5</p>

Source: Current research

These figures hold different meanings in financial institutions. While Fig 2 is about protecting and securing one's information as denoted by the locked padlock, Fig 3 highlights hanging up calls on scammers, Fig. 4 highlights caution as it stand for a phishing scam whereby the rat stands for someone who is attracted to the cheese (an enticing offer) but falls into the trap, which is a security risk, and finally, Fig 5 indicates a warning for one to either stop an activity, be cautious with transactions or halt a potential action. In all, these images, along with the colours have attached meanings to suspicious transactions, potential scams and the importance of security measures.

4.2.7 Common lexis

The data also showed the use of common lexis as seen below:

a) Fraud alert terminology: 'suspected fraud cases', 'suspicious activities', 'fraudsters', 'scam', 'unsecured websites', phishing, activity, 'security', 'scammers', 'clickbait', 'something fishy' etc.

b) Security/protection linguistic elements: 'secure your account', 'protect your information', 'safeguard your identity', 'keep it private', 'secret details', 'don't reveal, keep your card and pin information secure', 'don't click on any links', 'don't click or share', 'click with caution' etc

c) Acronymic formations: BVN, POS, CVV, PIN, OTP

Terminologies for fraud alerts refer to unique language and vocabulary items used to describe various aspects of fraudulent activities. They are important as their understanding is crucial for fraud prevention, detection, investigation, education and awareness. For example, the terms "suspected fraud cases", "suspicious activities", "scam", "phishing", and "clickbait" imply deceitful or unauthorised actions and illegitimate activities. Perpetrators, the specific individuals or groups committing fraud, are called fraudsters and scammers. "Unsecured websites" and "something fishy" suggest potential weaknesses or red flags and thus show customers' vulnerabilities. Threats are captured by the terms "phishing", "scam", and "clickbait", which all highlight specific tactics fraudsters use.

Further, bank fraud alerts equally deploy certain language elements that convey important security and protective measures. For instance, account protection activities are captured in the use of "secure your account", "protect your information"; identity safeguarding are seen in "safeguard your identity", and "keep it private"; confidentiality is in "don't reveal secret details", "keep card and PIN information secure" while caution with links is aptly captured in "Don't click on links", "click with caution".

These clear and direct language uses not only allow individuals to understand security best practices and take necessary precautions, but they also help to raise awareness about security risks, encourage safe online practices and protect sensitive information. Then the acronymic formations BVN (Bank Verification Number), POS (Point of Sale), CVV (Card Verification Value), PIN (Personal Identification Number) and OTP (One-Time Password) are commonly used and are crucial for secure financial transactions, identity verification and protection of sensitive information.

4.2.8. Salutation and personalisation elements

Bank alerts also use salutation and personalisation language resources. These greetings and politeness, such as 'Dear' and "thank you for banking with us"; the use of the customer's name (Mary); the inclusion of the first and last few digits of the affected account 003*****908), the account holder's name (Mary-Jane Marks); tailored messages (Your account has been credited/debited), transaction amount (Debit Amt: ₦5,000) and either a formal/informal tone are language resources that enable banks to create a personalised connection, a respectful tone, reflect politeness, build trust, enhance customer engagement and provide relevant information. This finding corroborates the studies of Balfageeh (2016) that personalisation is a feature deployed by banks to appeal to customers and that of Ayeni on the use of politeness as a discursive strategy by banks to engage customers. The study also agrees with Ayeni (2020) that inclusion is a banking strategy for customer engagement, however, only a minute use of inclusion was discovered ("Together, we can conquer fraud") as the cases

of “our” and “us” identified indicate exclusion and refer solely to the bank or service providers (“Keep your records with *us* up to date at any of *our* branches”, “Contact *us*...”, *we* are aware that some....”); so the customers are just being directed to reach out to the bank or perform a particular action.

4.2.9 Peculiar syntactic structures

These fraud alerts comprise varied syntactic structures. Some patterns include simple sentences (“Thank you for banking with us”; “Stay secure online”), compound (“They pretend to be our representative and ask for sensitive information to help solve your problems”), few cases of subordination (“If you think you have been a victim of fraud, please call our help desk”), interrogatives (“Suspect anything fraudulent?”), imperatives (“Don’t respond to such messages”), exclamations (“Beware!”) and phrases (“12 scams of Christmas”), etc.

The simple sentences represent clear and direct language with an underlying tone of urgency that enables customers to easily understand messages; likewise, the compound sentences, which are also important for joining two related ideas to provide additional information. The complex sentence, though less common, allows banks to provide specific conditions (e.g., “If you receive a suspicious alert...be cautious”).

4.2.10 Intertextuality and interdiscursivity

The data also reflected the use of intertextuality and interdiscursivity features as texts drew on or echoed other texts (intertextuality) and also indicated a blend of different discourses (interdiscursivity). For example, the text extract below is clearly indicative of these patterns:

“There was a successful login to
your Zenith mobile Account.
Please see login details below:
Friday, 4, 2023, 10:08:42 pm
If you did not login to your....
kindly contact ZenithDirect.....”

This message draws on the standard structure of bank alerts and cybersecurity notifications that customers may have encountered earlier. So, we have an implicit reference to a

previous interaction with the account that customers have seen before or a standard structure of bank alerts as captured in “There was a successful login”, “If you did not login...” and the potential link to support through the use of “ZenithDirect”. These texts reflect formats that indicate transactions or activity from an official and routine fraud alert communication. In other words, these linguistic resources echo standard structure and practices of cybersecurity notifications within financial institutions. Then interdiscursivity as reflected in the text shows a blend of different discourse types, as found in the use of the technical discourse “successful login”, “login details”; and the timestamp: “Friday, 4, 2023, 10:08:42 pm”, which all point to a system generated report of an activity; the security discourse that indicates an implicit warning, “if you did not login...” suggesting a potential unauthorised access, and a customer service discourse in the use of “kindly contact ZenithDirect” indicating a polite, service-oriented tone common in customer support communication. These intertextuality and interdiscursivity resources combine to help customers make sense of the new information by connecting the current information to what they already know, recognising legitimacy and authority, understanding consequences and engaging appropriately. This finding aligns with that of Balfageeh (2016) in his identification of intertextuality and interdiscursivity as features of banking interactions.

Conclusion

This study investigated the dynamics of the discourse used in online fraud alerts of Nigerian banks. The Genre Theory, a framework that engenders an understanding of the specific characteristics, linguistic elements and communicative strategies/purposes within a discourse community; and in this case, the context of Nigerian banks was deployed. 22 digital fraud alert posters from UBA, First Bank, Zenith Bank and Access Bank constituted the data. To this end, the findings reveal that Nigerian banks, in line with the communicative purposes of digital fraud alerts, use directness, conciseness and clarity as well as common syntactic structures for effective

communication and to ensure that recipients quickly grasp the nature of the alert. Other discursive strategies discovered include the use of actionable language, security-focused lexis, new media discourse, personalisation and educational elements. The use of these language resources highlights digital fraud alert posters as a warning and advisory genre aimed at preventing fraud and protecting bank customers.

The results indicate, therefore, that online bank fraud alerts are generic elements that highlight unique communicative practices as an institutional warning and advisory genre in Nigeria. That is to say that these alerts are crafted

with peculiar discursive elements based on their communicative purposes of warning and prevention, instruction and guidance, building trust and institutional credibility, legal and regulatory compliance, as well as raising awareness and educating customers. The findings from this study are very important in providing valuable insights into efforts to protect bank clients, enhance the efficiency of bank fraud prevention measures and foster a more resilient financial ecosystem. The study's significance stems from its implications for bank clients, banking institutions, and financial and fraud experts.

References

- Amy D. (1993). Generalizing about genre: New conceptions of an old concept. *College Composition and Communication*, 44 (4), 573-585.
- Ayeni, B. (2010). Winning the customers over and again: Investigating discourse features in Nigeria banking interactions. *International Journal of English Language Studies (IJELS)*. 2 (3), 45-59.
- Badejo, B.A., Okuneye, B.A. & Taiwo, M.R. (2017). Fraud detection in the banking system in Nigeria: challenges and prospects. *Shirkah Journal of Economics and Business*, 2 (3), 255-282.
- Balfaqeeh M (2016). It's all about you...:The discourse of banking in the UAE. *Globe: A Journal of Language, Culture and Communication*, 3, 10-27.
- Blommaert, J. (2005). Discourse: A critical introduction. *Cambridge University Press*.
- Breeze, R. (2012). Corporate discourse. *Continuum*.
- Buckley, R. P., Arner, D. W. & Barberis, J. N. (2016). The evolution of fintech: A new post-crisis paradigm? *Georgetown Journal of International Law*, 47(4), 1271-1319.
- Carter, E. (2023). Confirm not command: Examining fraudsters' use of language to compel victim compliance in their own exploitation. *The British Journal of Criminology*, 63, 1405-1422
- Furnell, S. & Emm, D. (2008). Phishing: Can We Spot the Signs? *Computer Fraud & Security*, 3, 10-15. [https://doi.org/10.1016/S1361-3723\(08\)70023-1](https://doi.org/10.1016/S1361-3723(08)70023-1)
- Gaffaroglu S. & Alp S., (2023). Detecting frauds in financial statements: A comprehensive literature review between 2019 and 2023 (June). *Press Academia Procedia (PAP)*, 18, 47-51.
- Gillen, J. (2016). Narratives of fraud victims: Identity, emotion and blame. *Discourse & Society*, 27(5), 512-527.
- Harte, B. K. and McHone, S.P. (2019). Discourse fraud analysis: A new paradigm for forensic and investigative accounting. *Journal of Forensic and Investigative Accounting*, 11(3), 425-439.
- John M. S (1990). Genre Analysis: English in academic and research settings *Cambridge University Press*
- Miller C. R. (1984). Genre as Social Action. *Quarterly Journal of Speech*, 151-167
- Nwanaka, C. (2022). Overview of the concept of fraud in the Nigerian banking system, *BW Academic Journal*, 1(1), 32-38.
- Olajimbiti, E. O. (2018). Discourse pattern, contexts and pragmatic strategies of selected fraud spam. *Crossroads. A Journal of English Studies*, 21(2), 53-63.
- Olaoye, C.O. & Adekola, D.R. (2014). Analysis of Frauds in Banks: Nigeria's Experience. *European Journal of Business and Management*, 6 (3), 190-99.
- Osisanwo, A. & Olaniyi, T. (2021). Discourse and visual strategies in framing internet fraudsters in selected Nigerian newspapers. *Ibadan Journal of English Studies (Special Edition)*. 16,132-156.

- Owolabi, S. A. (2010). Fraud and fraudulent practices in Nigeria banking industry. *African Research Review, An International Multi-Disciplinary Journal*, 4 (3b), 240-256.
- Pousttchi, K. & Dehnert, M. (2005). Exploring the adoption of mobile push services for financial news. Proceedings of the International Conference on Mobile Business (ICMB), 1–6.
- Rahman A.U. (2021). A Critical review of fraud discourse - A case study of Pakistan. *ECOSAI CIRCULAR*, Spring Issue, 48-59
- Sun, H., Li, J. and Zhu X. (2023). Financial fraud detection based on the part-of-speech features of textual risk disclosures in financial reports. *ScienceDirect, Procedia Computer Science* 221, 57–64