Cyber Risks in Microfinance Digitization: Exposures and Preventions among Female Headed Farm Households in Southern Nigeria

V. C. Ugwuja and O. M. Adesope

ABSTRACT

Digital finance is widely regarded as one of the most effective means of financially empowering women and increasing their financial inclusion. On the other hand, cybercriminals are constantly looking for new ways to exploit vulnerabilities and developing ever more sophisticated attack methods. As a result, the cyber risk exposures and prevention of female heads of farm households in Southern Nigeria were investigated in this paper. Unsuccessful transactions by mobile applications and POINT OF SALES (POS) terminals were often encountered by female heads, and yet their money was debited, and it took a long time for their money that was debited from unsuccessful transactions to be reversed. Avoiding lonely ATMs and not going to the ATM during late hours, ignoring emails and text messages instructing them to provide online banking details, no longer using birthdates, addresses, and other words or numbers that would make it easier for attackers to figure out their passwords, and not using the same passwords for all their different accounts were the most common cybersecurity measures used by female heads. Access to digital financial products and services was influenced by factors such as marital status, household size, business experience, internet access, possession of an ICT device, and perceived security risks. These findings call for interventions by the Central Bank of Nigeria (CBN) through policies that will improve consumer education and reduce vulnerabilities, especially among women. The CBN should also develop a forum that is easily accessible to customers for filing complaints, and erring banks should be sanctioned.

Keyword: Cyber risks, Cybersecurity, Digital Financial Products, Southern Nigeria.

I. INTRODUCTION

Microfinance has been recognized as the most viable, effective, and result-oriented tool to empower poor people, in particular women financially. However, there are a number of problems and obstacles to the success of microfinance as an industry. Sustainability, outreach and impact are the main issues. Thousands of microfinance institutions worldwide realize that the best solution for the scale-up and ensuring maximum coverage and sustainability of MFIs is to leverage technological advantages, especially Information and Communication Technology (ICTs). Microfinance providers use ICT in their day-to-day activities in many ways. These include fund transfers, mobile payments financing, micro-financing platforms, Client Notification systems, savings, farmers’ microinsurance systems, SMS marketing customer enrollment, micro insurance product marketing including life and weather insurance, mobile phone claims and field loan analysis [1].

The key issue for empowering women is access to financing. [2] indicated that 40.9% of Nigerian women have no bank account compared with 32.5% of men. Women are usually excluded both intentionally and because of factors which cause them to be disadvantaged, such as lack of freedom of movement or low levels of education, from the domain of outside information. For women outside the world, ICT opens a direct window. Information fluctuates without distortion or censorship [3]. The financial services sector is a primary driver for communications and network technology and ICT enables better financial inclusion. ICT can also enhance the capacity of the government to supervise and evaluate rural clients’ financial services and to design efficient rural sector financial policies and regulations [1].

Many studies have shown that female households have a higher dependency burden than other households. [4] as cited in [5] shows that in Panama, only certain categories of female-heads such as widows, and female-heads with unmarried partners are particularly disadvantaged in both income and non-income dimensions of poverty compared to male-headed households. [6] also showed that female-headed households have worse social, economic, and demographic features compared to male-headed counterparts and are thus more likely to be poor. Women-led farm households are usually engaged in small-scale farming in rural communities, trapped in their own impoverished world. They frequently lack access to assets and family property, contributing to an already precarious economic situation. Micro-finance through the use of ICT is a comprehensive tool that renders services such as savings, micro leasing, small loans, micro insurance and payment transfer to low-income people such as female heads of households.
Digital financial products and services are accessed electronically. Electronic banking characteristics do not match those of the conventional financial sector. Due to more differentiated risks in Internet banking and the impact of an intensification of risk, it would become more difficult to avoid risks in on-line finance [7]. Risk control and management procedures need to be strengthened in light of the risks in digital finance. Otherwise, electronic banking will be seriously endangered. Since banks are increasingly relying on IT and the internet to run their business and interact with the markets, they must be more sensitive and discerning in understanding and recognizing the size and intensification of cyber risks. Cyber-risk refers to risks arising from the use and transfer of electronic data, including technological instruments such as the Internet and networks. It also includes physical damage that may arise from cyber attacks, misusing data, liability for data storage, accessibility, integrity, and confidentiality of electronic information, regardless of whether it is related to individuals, firms or governments [8].

Such risks as experienced by banks are classified into several clusters, such as security risks, legal and ethical risks, reputational risks, operational risks, money laundering risk, strategic risks, cross border risks and traditional risks [9]. These risks are in different ways faced both by financial institutions and their customers. There are several dimensions of risk that contribute to the magnitude of risk perceived by consumers when using online banking services. The risks perceived by customers are: (a) social risk, which refers to the utility or approval that people receive when consuming recognized products or services within their own social groups; (b) Financial risk is one of the underlying dimensions of perceived risk that refers to the risk associated with the expected potential monetary loss in the form of erroneous money transfer and incomplete knowledge about transaction costs. (c) The functional dimension of risk refers to the core benefit and basic utilities of a good or service. It includes aspects such as quality, uniqueness, ease of use, reliability, and durability of the product [10] as cited [11]. Individual risk expresses how 'risk-averse' people tend to be or try to avoid any form of risk, and how 'risk-friendly' people enjoy or expectantly tolerate the associated emotion or uncertainty [12] as cited in [11]. (d) Security risk is related to customer account hacking.

Limited research is done on risk exposures and risk management strategies adopted by women, especially female-headed farm households, on accessing digital financial products and services.

Against this background, this study will identify basic elements of assessing, controlling and monitoring electronic banking risks faced by microfinance customer clients in Southern Nigeria. The study will lay a foundation for long term development of a sustainable online financial inclusive system, and also long term social gain and cost savings for both banks and their customers.

Nigeria is bedeviled by poverty, inequality, unemployment and youth restiveness. Therefore, the hypothesis that is aimed at identifying influential factors on access to digital financial products and services in order to provide useful information on inclusive financial services is of the utmost importance. Policies that will scale this up will be a win-win situation for Nigeria. Most importantly, female headed-households are usually socially excluded. It is therefore pertinent to develop a study that assesses the usage of digital finance by this class of women who are associated with poverty in order to develop policies that will engender alleviation of their poor status. Hence the need for this study.

A. Objectives of the Study
The specific objectives of the study were to:

i) identify digital financial products and services accessed by female farm household heads in Southern Nigeria.

ii) identify cyber risks experienced by female farm household heads in Southern Nigeria.

iii) examine the preparedness of the respondents towards cyber security in the study area.

iv) determine the socio-economic factors and perceived security risks that influence access to digital financial products and services in the study area.

B. Hypothesis of the Study
Ho₁: Socio-economic factors and perceived risks of the respondents have no significant influence on access to digital financial products and services in Southern Nigeria.

II. METHODOLOGY

A. Study Area
The area of study was Southern Nigeria. It occupies a total land area of 193,347 km² and has a total population of 64,978,376 persons [13]. Nigeria has six geo-political zones in which three geo-political zones make up Southern Nigeria. It comprises of 17 states out of 36 states of Nigeria. It boasts diverse vegetation belts ranging from Nigeria's largest rain forests to mangrove swamps, savannahs, mountains, and waterfalls teeming with rare animals, endangered species, and unusual plant families, making it one of the world's richest biodiversity hotspots, attracting both scientists and tourists. Niger Delta region is located in Southern Nigeria. It is where most of the country's oil is located.

B. Sampling Technique and Sample Size
The respondents for this study were chosen using a multistage sampling procedure. Southern Nigeria is divided into three geopolitical zones: Southeast, which consists of five states; Southwest, which consists of six states; and South-south, which consists of six states. Two states were randomly selected in each geopolitical zone, making it a total of six states in the study. These states were Abia, Enugu, Bayelsa, Rivers, Ekiti and Ondo. In each selected state, two Local Government Areas(LGAs) were purposively selected making it a total of 12 LGAs. In Abia, the LGAs were Umunhua North and Umunhua South, in Bayelsa the LGAs were Yenagooa and Sagabama, in Enugu the LGAs were Orji River and Nkanu West, in Rivers the LGAs were Ikwere and Khana, in Ekiti the LGAs were Ikere and Ado-Ekiti, while in Ondo, the LGAs were Akure North and Ifedore. Two farming communities were purposively selected from each LGA making it 24 farming communities for the study. Purposive selection was made based on the presence of financial institutions in the farming communities. In such selected community, there was a purposive selection of 10 female farm household heads that access digital financial products,
and 10 that do not access digital financial products. That made it a total of 240 of them that access digital financial products, and another 240 that do not access financial products. Making it a total of 480 female farm household heads for the entire study.

C. Data Collection

The primary data were collected through the use of a structured questionnaire and oral interview. The study used two sets of questionnaires; the first set was for female household heads who use digital financial products. The second set of questionnaires was distributed to female heads of households who do not have access to digital financial products.

D. Data Analysis

The data were analyzed using two distinct approaches: descriptive statistics and inferential statistics such as binary logistic regression.

E. Model Specification for Binary Logit

Given that the dependent variable is dichotomous, a binomial logistic regression model was used: 0 when a female household head does not have access to digital financial products and 1 when she does. The predictor variables are a collection of indicators of female household heads' socioeconomic status and perceived risk. They include both categorical and continuous variables. Assume that Pj is the probability that the jth female household head has access to digital financial products. We assume Pj is a Bernoulli variable whose distribution is determined by the vector of predictors X, so that:

\[ P_j(X) = \frac{e^{\alpha + \beta X}}{1 + e^{\alpha + \beta X}} \]  

(1)

The logit function to be estimated is then written as:

\[ \ln\left(\frac{P_j}{1-P_j}\right) = \alpha + \sum I \beta_i X_{ij} \]  

(2)

The logit variable \(\ln(P_j/(1-P_j))\) represents the natural logarithm of the probability that a female household head has access to digital financial products. The coefficient estimates of \(\beta\) gives the change in the log-odds (logarithm of relative probabilities) of the outcome—here = 1—for a one-unit increase in the independent variable, all other independent variables remaining constant. Maximum Likelihood (ML) is used to estimate logit regressions rather than Ordinary Least Squares (OLS). ML calculates coefficient estimates that maximize the likelihood of the sample data set being observed.

The binary logit model to be estimated is specified as follows:

\[ C_{ij} = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \beta_5 X_5 + \beta_6 X_6 + \beta_7 X_7 + \beta_8 X_8 + \beta_9 X_9 + \beta_{10} X_{10} + u \]  

(3)

Cij = Dummy = 1 if the female household head is accessing digital financial products, and 0 otherwise.

X1 = Age (Years).
X2 = Household Size (Number).
X3 = Educational Status (Years).
X4 = Farming status (Full-time= 1, Part-time= 0).
X5 = Cooperative Membership (Dummy; Yes =1, No=0).
X6 = Business experience (Years).
X7 = Internet access (Dummy; Yes= 1, No= 0).
X8 = Ownership of ICT device (Dummy; Yes= 1, No= 0).
X9 = Annual income (Naira).
X10= Perceived security risk (Dummy; Yes= 1, No= 0).

u = stochastic error term.

III. RESULTS AND DISCUSSION

A. Digital Financial Products Accessed by Female Heads of Farm Households in Southern Nigeria

The response of female heads of farm households to access to digital financial products is depicted in Fig. 1. The overwhelming majority (98.7%) of respondents indicated that they use ATM/Debit cards, which corresponds to the report of [14] which stated that 76.2% of Nigeria's banked population owns ATM/Debit cards. SMS Alert services were also heavily utilized by respondents (98.3%). The majority of female household heads indicated that they use USSD Banking Codes (92.9%), Point of Sale (79.1%), Balance inquiry (85.8%), and Online Fund Transfer (65.3%).

Additionally, analysis of the results indicates that respondents use these digital financial products on a moderate basis: email alerts (51.0%), online bill payment (51.0%), e-statements (49.8%), and online purchases (43.5%). These are the least accessed products, according to respondents: remittances (31.0%), online loans (21.8%), online deposit accounts (20.9%), online savings accounts (7.1%), and micro insurance (4.2%). This corroborates [15] findings that the banked population in Nigeria has the least access to online savings accounts and insurance.

B. Cyber Risks Experienced by the Female Heads of Farm Households in Southern Nigeria

Table I contains responses from female household heads regarding cyber risks. The results indicated that approximately 54.0% of respondents agreed that whenever they used the bank's USSD code, they always received error messages prior to the transaction being completed. Around 49.0% of respondents indicated that their mobile app transactions were unsuccessful and yet their accounts were debited. Only 7.5% admitted that someone close to them used their ATM cards to withdraw money from their accounts without their knowledge. Only 2.9% stated that they were approached by criminals after withdrawing money from an ATM. About 39.7% indicated that they paid via POINT OF SALES (POS) terminal. The transaction was not approved, but money was deducted from their accounts. This implies that a substantial number of customers who pay at the point of sale are exposed to this risk. Around 14.6% indicated that they received a text message (SMS) requesting that they urgently provide their bank account information, and that money was withdrawn from their account after providing the account information. This is consistent with the findings of [16], who reported that the majority of their respondents were victims of cyber-attacks after disclosing their banking information via text messages. Around 7.9% of respondents reported receiving a call from an unknown person claiming
to be a bank customer representative, requesting their bank account information, which was subsequently provided, and money was withdrawn from their accounts. This finding is supported by the [17], which reported that the majority of common cyber-attacks are mostly caused by users disclosing personal information to fraudsters. Only 6.7% of respondents indicated they had been a victim of phishing, which means they received an email that looked identical to one from their banks requesting they urgently provide their bank account information via a link embedded in the email, which they did, and money was subsequently withdrawn from their accounts.

![Digital Financial Products accessed by Female heads of Farm Households](image_url)

Fig. 1. Digital financial products accessed by female heads of farm households.

| S/N | Cyber risks                                                                 | Yes (%) |
|-----|-----------------------------------------------------------------------------|---------|
| 1   | I received an email that appeared to be from my bank, requesting that I provide my bank account details as soon as possible via a link embedded in the email, which I did, and money was then withdrawn from my account. | 6.7     |
| 2   | I received a text message (SMS) requesting that I provide my bank account information as soon as possible, and after providing the information, money was withdrawn from my account. | 14.6    |
| 3   | I visited a malicious website on my system and that resulted to the exposure of my bank account details stored on the system and allowed criminals to withdraw money from my account. | 1.3     |
| 4   | Someone close to me used my ATM card to make a hidden withdrawal from my account. | 7.5     |
| 5   | I was approached by criminals who carted away with my money after withdrawing money from an ATM. | 2.9     |
| 6   | I received a text message saying that my ATM card has been de-activated and that to re-activate it I should call someone through a phone number provided in the message, which I did, and after providing my card details to the person for re-activation, money was withdrawn from my account. | 18.8    |
| 7   | I was trying to transfer money through my mobile application, the transaction did not go through due to network issues, but the money was debited from my account. | 49      |
| 8   | It took a long time for my money that was debited from unsuccessful transaction to be revised. | 38.1    |
| 9   | Every time I try to make use of my bank’s USSD code, I always get error messages before the transaction goes through. | 54      |
| 10  | I received an email that looks as if it is coming from my bank requesting that I urgently change my online banking password through a link provided in the email, which I did, and thereafter money was withdrawn from my account. | 3.3     |
| 11  | My phone was stolen, and I couldn’t carry out transactions on my online banking accounts due to my inability to receive the ONE TIME PASSWORD that my bank sends for every transaction. | 10.9    |
| 12  | I did shopping on a fraudulent shopping website, I entered my ATM/DEBIT CARD details and money was debited from my account without receiving what I paid for. | 2.9     |
| 13  | I made a payment at a POINT OF SALES (POS), and even though the transaction was rejected, yet the money was deducted from my account. | 39.7    |
| 14  | I received a call from an unknown individual claiming to be a representative from my bank's customer service department, telling me that my online banking account had been temporarily locked due to suspected unauthorized request for password change from me, and that I should provide my account login details so they can unlock the account, which I did, and thereafter money was withdrawn from my account. | 7.9     |
| 15  | After shopping successfully in an online website, afterwards I started receiving unauthorized charges on my account. | 0.8     |
| 16  | I used a public Wi-Fi Network to access my online banking account and thereafter my login details were stolen, and money was withdrawn from my account. | 0       |
| 17  | I entered my online banking account login details on a website that looks exactly like that of my bank and thereafter, my account was hijacked, and my money withdrawn. | 0.4     |
| 18  | I used someone else's system to access my online banking account and thereafter, my login details were stolen, and money was withdrawn from my account. | 0       |
| 19  | My phone got missing and before I could retrieve my line and get a new phone, money have been withdrawn from my bank account. | 0.4     |
| 20  | I helped somebody to withdraw money that s/he transferred into my account, without knowing that the transfer was from a hacked account. My account was blocked, and I was arrested by the police. | 0.8     |

Source: Author (2019).


C. Cybersecurity Measures Adopted by Female Heads of Farm Households

Table II shows the cybersecurity measures taken by female heads, with the following measures being the most popular:

1) I avoid isolated ATMs and late-hour ATM visits (94.1%);
2) I ignore and delete emails and text messages requesting that I provide my online banking information through any channel (93.7%);
3) I have discontinued the use of birthdates, addresses, and other words or numbers that make it easier for attackers to guess my password (90.0%);
4) I do not use the same password for all of my bank accounts (88.3%);
5) I exercise caution whenever I login to my online banking site to avoid prying eyes obtaining my account login information (87.4%);
6) I check my account history and balance on a regular basis to ensure that everything is in order (78.2%);
7) I contact my bank to verify any details I receive online or by text message about my online account (70.3%);
8) I no longer click on links found in suspicious-looking emails, regardless of how real they seem (69.9%); I cover the ATM keypad with my hand when entering my PIN (66.4%); I immediately notify my bank when I see unauthorized debit alerts (71.3%).

Female heads of farm households implemented the following cybersecurity initiatives in a moderate manner:

1) I always log out of my bank’s mobile application after completing a transaction (61.5%);
2) My mobile computer is password-protected (60.3%);
3) I only download apps from approved app stores (57.3%);
4) I always update my online banking applications when asked to do so (61.5%) (56.1%).

The following cybersecurity interventions were reported to be the least frequently used by respondents. Among them are the following:

1) I now use a PREPAID CARD for online purchases (8.8%);
2) I have a dedicated minimal savings account for online transactions (14.2%);
3) I have now used a reliable antivirus program to protect my mobile device/computer (22%).

| S/N | Cybersecurity Measures | %    |
|-----|------------------------|------|
| 1   | I take extra precautions whenever I want to access my online banking platform in order to keep prying eyes from gaining access to my account login information. | 87.4 |
| 2   | I disregard and delete emails and text messages requesting my online banking information via any channel. | 93.7 |
| 3   | I've stopped clicking on links found in suspicious-looking emails, regardless of how genuine they seem to be. | 69.9 |
| 4   | I contact my bank to double-check any information I receive about my online account from websites or text messages. | 70.3 |
| 5   | I check my account balance and history on a regular basis to ensure that everything is in order. | 78.2 |
| 6   | I've discontinued the use of birthdates, addresses, and other words or numbers that make it easier for attackers to guess my password. | 90.0 |
| 7   | For all of my bank accounts, I don't use the same password. | 88.3 |
| 8   | I avoid using isolated ATMs and I avoid going to the ATM during late hours. | 94.1 |
| 9   | I now protect my mobile device with reputable mobile security software. | 22.0 |
| 10  | I've switched to two-factor authentication (PIN and OTP) for mobile banking. | 43.1 |
| 11  | I immediately dial my bank whenever I lose or misplace my ATM card to freeze my account. | 64.4 |
| 12  | I installed antivirus software to prevent viruses, key loggers, and other malicious programs from compromising my computer. | 28.9 |
| 13  | I never conduct online transactions through unencrypted private wireless networks or public Wi-Fi. | 23.4 |
| 14  | I always make online purchases through well-known e-commerce websites that begin with https:// rather than http://. | 25.1 |
| 15  | I only download applications from authorized app stores. | 57.3 |
| 16  | I instantly notify my bank when I see unauthorized debit alerts. | 64.0 |
| 17  | I make all online purchases using a PREPAID CARD. | 8.8 |
| 18  | I set aside a small savings account specifically for online transactions. | 14.2 |
| 19  | I disallow web browsers from storing my online banking login details. | 0.0 |
| 20  | I make sure my bank website is legitimate before I enter my login details. | 8.8 |
| 21  | I use dedicated system to access my online banking accounts. | 52.7 |
| 22  | I access my online banking accounts through a dedicated browser. | 44.4 |
| 23  | I always update my online banking applications whenever I'm prompted to do so. | 56.1 |
| 24  | My mobile device is password-protected. | 60.3 |
| 25  | I use strong password for my online banking account. | 64.0 |
| 26  | I cover the ATM keypad with my hand while entering my PIN. | 66.4 |
| 27  | I keep my ATM card safe and protect the card details from strangers and even people close to me. | 65.7 |
| 28  | I always make sure that my bank website starts with https:// instead of http before I log into my online banking account. | 37.2 |

Source: Author (2019).

D. Determinants of Access to Digital Financial Products by Female Heads of Farm Households in Southern Nigeria

A binary logistic regression was used to determine the effect of socioeconomic variables on female heads of farm households’ access to digital financial products in Southern Nigeria, as shown in Table III. The dependent variable (access to digital financial products) was defined as follows: accessed = 1, did not access = 0. The model is statistically significant, indicating that the explanatory variables estimated reliably distinguished female heads who accessed digital financial products from those who did not (Chi-square = 440.063, P = 0.000). The Nagelkerke R-square value of 0.801 indicates that the combined effects of all the independent variables in the model explained 80.1 percent of the variation in access to digital financial products.
Six of the ten explanatory variables examined in the model were statistically significant in terms of accessing digital financial products: marital status, household size, business experience, internet access, ownership of an ICT device, and perceived security risk.

The marital status coefficient is positive and statistically significant at 10%. This finding implies that married female heads of households are more likely to use digital financial products. This may be possible as a result of their husbands’ positive influence. The household size coefficient is positive and statistically significant at the 5% level of probability. This means that for every additional unit of household size, the likelihood of accessing digital financial products increases by 17%. At 10% level of significance, business experience has a statistically significant negative coefficient (=-0.044). The findings suggest that female heads with a long history in business are less likely to use digital financial products. This could be because people who cling to old habits often struggle to embrace new ones. Internet connectivity is a significant predictor of access to digital financial products. According to the study, female heads of farm households with internet access are more likely to use digital financial products. This is consistent with [18] findings that internet access is a significant determinant of internet banking adoption in India. Ownership of an information and communication technology device is statistically significant (P=0.001) and has a positive coefficient (3.898). This finding indicates that female heads who own ICT devices such as phones and tablets are more likely to access digital products. This finding is consistent with expectation, as accessing digital financial products requires the use of an ICT device. Perceived security risk is statistically significant at 1% with a negative coefficient, implying that female heads who are risk averse are less likely to access digital financial products. This is consistent with [19] findings that security risk has a negative effect on the intention to use internet banking.

### ACKNOWLEDGEMENT

We would like to thank the female heads of farm households who willingly participated in the study, extension agents and field enumerators who conducted the survey. The project recognizes the support of the host University, University of Port Harcourt, and most importantly, the AXA Research Fund Community for funding this research.

### FUNDING

This study was funded by AXA Research Fund Community, an AXA Group's Science Philanthropy Initiative in Paris, France.

### REFERENCES

1. World Bank. ICT enabling rural financial services and micro-insurance for smallholders [Internet]. e.forum. 2013 [cited 2016 Oct 2]. Available from: http://www.ictinagriculture.org/sourcebook.
2. Enhancing Financial Innovation and Access (EFInA). Access to Financial Services in Nigeria 2018 Survey. [Internet]. 2018 [cited 2019 Feb 2]. Available from: www.efina.org.
3. Suman J. ICTs And Women’s Empowerment: Some Case Studies from

### TABLE III: DETERMINANTS OF ACCESS TO DIGITAL FINANCIAL PRODUCTS BY FEMALE HEADS OF FARM HOUSEHOLDS IN SOUTHERN NIGERIA

| Variables               | Coeff  | Std. Error | Z-Stat  | P-Values |
|-------------------------|--------|------------|---------|----------|
| Age (X1)                | 0.024  | 0.035      | 0.669   | 0.504    |
| Marital status (X2)     | 1.199  | 0.696      | 1.722   | 0.085    |
| Household Size (X3)     | 0.168  | 0.077      | 2.185   | 0.029    |
| Educational Status (X4) | 0.022  | 0.054      | 0.396   | 0.692    |
| Farming Status (X5)     | 21.304 | 2335.470   | 0.009   | 0.993    |
| Ownership of ICT device | -0.401 | 0.343      | -1.167  | 0.243    |
| Membership (X6)         | -0.044 | 0.026      | -1.689  | 0.091    |
| Business Experience     | -0.044 | 0.390      | 3.418***| 0.000    |
| Internet access (X7)    | 1.300  | 0.380      | 3.331***| 0.000    |
| Ownership of ICT device | 3.898  | 1.170      | 3.331***| 0.000    |
| Perceived Security Risks| -0.755 | 0.210      | -3.591***| 0.000    |
| Constant                | -26.968| 2335.471   | -0.012  | 0.991    |
| Omnibus Test Chi Square | 440.063|           |         |          |
| Prob>chi square          | 0.000  |            |         |          |
| Nagelkerke R-square     | 0.801  |            |         |          |

*** Significant at 1% level, ** Significant at 5% level, *Significant at 10% level.
India [Internet]. LakshmiBai College, Delhi University; Available from: unpan1.ian.org/intrado/groups/public/documents/apcity/.

[4] Fuwa N. “The Poverty and Heterogeneity among Female Household Heads Revisited:The Case of Panama.” World Dev. 2000;28(8):1515–42.

[5] Ramaprasad R. Female-Headed Households and Poverty: Evidence from the National Family Health Survey. Terry College of Business, The University of Georgia, Athens, GA.; 2009.

[6] Barros, R., Fox, L., &Mendonca R. “Female-Headed Households, Poverty, and the Welfare of Children in Urban Brazil.” Econ Dev Cult Change. 1997;45(2):231–57.

[7] Gunjun Y. Risk types and risk amplification of online finance. Inf Technol J. 2013;12(3):494–7.

[8] Financial Services Sector Coordinating Council. Purchasers’ Guide to Cyber Insurance Products [Internet]. 2016 [cited 2017 Jun 10]. Available from: www.fsccc.org.

[9] Virender SS. Risks in E-Banking and Their Management. Int J Mark Financ Serv Manag Res. 2012;1(9):164.

[10] Sääksjärvi, M., & Lampinen M. Consumer perceived risk in successive product generations. Eur J Innov Manag. 2005;8(2):145–56.

[11] Nadine, H., Klaus-Peter, W., Barbara, S., Lars, P & Martin K. The influence of consumers’ risk attitudes and behavior on the adoption of online banking services. J Mark Trends. 2010;11(1):7–16.

[12] Slovic P. Risk as Analysis and Risk as Feelings: Some Thoughts about Affect, Reason, Risk, and Rationality. In: National Cancer Institute workshop on Conceptualizing and Measuring Risk Perceptions. Washington D.C: 2003.

[13] National Population Commission. Nigeria 2006 Population Census Arranged by State. Abuja, Nigeria; 2006.

[14] Enhancing Financial Innovation and Access (EFInA). Access to Financial Services in Nigeria 2014 Survey [Internet]. 2014 [cited 2018 Jun 4]. Available from: www.efina.org.

[15] Enhancing Financial Innovation and Access (EFInA). Access to Financial Services in Nigeria 2016 Survey [Internet]. 2016 [cited 2018 Jun 16]. Available from: www.efina.org.

[16] Omodunbi B.A, Odiase P.O, & EA. Cybercrimes in Nigeria: Analysis, Detection and Prevention, Journal of Engineering and Technology, J Eng Technol. 2016;1(1):27–42.

[17] National Cybersecurity Center (NCC). Common Cyber attacks: Reducing the Impact. [Internet]. 2016 [cited 2018 Jan 18]. Available from: www.cyber-center.org.

[18] Vijay M. Determinants of Internet Banking Adoption: An Empirical Evidences from Indian Banking. Indian J Commmer Mang Stud. 2011;2(1):4–25.

[19] Fadare O. A Survey on Perceived Risk and Intention of Adopting Internet Banking. J Internet Bank Commmer. 2016;21(1):1–21.

Dr Ugwuja Vivian Chineo is a Senior Lecturer in the Department of Agricultural Economics and Extension, University of Port-Harcourt, Rivers State, Nigeria. She obtained her B.Agri (Animal Science) from University of Nigeria, Nsukka and was the best graduating student for the year 2001. She obtained her M.Sc in Agricultural Economics from Rivers State University of Science and Technology in 2010, and her doctorate degree in Agricultural Finance and Project Analysis from the University of Nigeria, Nsukka in 2016.

Her research interests include rural development, microfinance, digital finance, and cybersecurity. She has practical experience with community youth and women cooperatives where she has been involved in enterprise development for the youths and women. She is currently the chairperson, UNIPORT CHORA SEEPOR/Fadama Community Association, a World Bank assisted project. She was a Postdoctoral research fellow in Cybersecurity from 2017-2019, awarded and sponsored by AXA Research Fund Group, honoured to be the first Nigerian awardee.

She has published a chapter in a book, many journals (national and international) and conference proceedings, she has attended conferences, workshops and trainings. She is a member of Nigerian Association of Agricultural Economists (NAAE) and Organization for Women in Science for the Developing World (OWSD). She also belongs to so many committees both in the university and religious bodies.

Olufemi Martins Adesope is a Professor of Agricultural Extension in the Department of Agricultural Economics and Extension, University of Port Harcourt, Nigeria with 25 years teaching, research, and community service experiences. He is the Associate Dean, School of Graduate Studies. He has held various administrative responsibilities in different capacities as Head, Department of Agricultural Economics and Extension, Associate Dean of the Faculty of Agriculture. He was the Chairman, Graduate Studies Committee of the Department of Agricultural Economics and Extension, University of Port Harcourt. He is the Chairman, Faculty of Agriculture Research and Training Committee, University of Port Harcourt. He was the Assistant Director, Centre for Research Management and Development in the University of Port Harcourt where he has facilitated workshops, scholarship, fellowship programmes for staff of the University of Port Harcourt. He was instrumental to producing the Mentorship policy document for the University of Port Harcourt. Professor Adesope has several publications in books, journals, chapters in books, conference proceedings, and monographs. He is on the Editorial Board of several Academic journals.