Gender, Cybersecurity and Fraud in DFS

Wechsler, M[1] and Siwakoti, S[2]

Abstract

This paper explores how issues and malfeasances relating to cybersecurity and cyber fraud differ based on gender, primarily focusing on women, in relation to the use of mobile-phone centric digital financial services (DFS) in developing countries in Africa and South Asia.

We find that women within the scope of our study may be more susceptible than men to malfeasances and other concerns related to cyber risks and cyber fraud as a result of inequalities and gender gaps that exist within developing countries. Women consistently ranked behind men with regard to access to, use of and experience with information and communication technologies, ownership of mobile hardware and DFS. Women were perceived to possess lower digital and language literacy rates and subjected to limiting social, cultural, religious and legal barriers. These factors often tied them to roles in private spaces, such as the family home. As such, access to important peer knowledge networks which disseminate timely information about cybersecurity and fraud issues was limited, which often occur in public spaces (such as the workplace, in the marketplace and social settings). As a result, women's overall cyber awareness and cyber hygiene levels would likely to be lower than men, including their capabilities to combat social engineering related fraud which appears to present a formidable challenge in developing countries.

Presently, a paucity of gender-disaggregated data exists and/or is available publicly related to information and communications technology and cybersecurity. Findings from relevant available data were supplemented by interviews conducted with regional and local experts and consultants in the field.

With faith in the security of financial systems and process being the mainstay of user adoption and use of services, we find that the distinct lack of quantitative and qualitative research on gender differences in susceptibility to fraud, social engineering attacks and cyber-attacks is a siren cry for additional focus and funding of this important issue by academic institutions, donor communities, and think tanks. Furthermore, mobile network operators, digital financial services providers and related governmental authorities and agencies are encouraged to increase their outreach to women, especially in rural areas, to increase their levels cyber awareness and hygiene and to address rapidly increasing cybercrime.

[1] Michael M. Wechsler, A. Research Scholar: Digital Financial Services Observatory, Columbia Institute for Tele-Information, Columbia University, New York.
[2] Samikshya Siwakoti, Research Staff Digital Financial Services Observatory, Columbia Institute for Tele-Information, Columbia University, New York

Table of Contents

1 Overview 4
1.1 Introduction 4
1.2 Scope and Methodology 4
1.3 Introduction to Digital Financial Services (DFS) 6
1.4 Cybersecurity and Fraud in DFS with a Gender Lens 7
2 Gender Divides 10
2.1 The Digital Gender Divide: Mobile Access, Handsets and Usage 10
2.1.1 Mobile Coverage and Mobile Internet Access 10
2.1.2 Ownership and Sharing 11
2.2 DFS Onboarding, Account Ownership and Literacy Levels 17
2.2.1 DFS Onboarding 17
2.2.2 Financial Literacy and Account Ownership 18
2.2.3 Education, Literacy and Numeracy 19
2.2.4 Technical Literacy 21
2.3 Social, Cultural, Economic and Gender Specific Divides 23
2.3.1 Social, Cultural and Economic Divide 23
2.3.2 Gender Imbalances, Women's Confidence and Sexual Harassment 26
3 Cybersecurity and Fraud in DFS: View with a Gender Lens 28
3.1 Cybersecurity: Regional Perspective 29
3.2 Cybersecurity Issues, Awareness and Practices 30
3.3 Social Engineering 33
3.3.1 Social Engineering Methods and Techniques 33
3.3.2 Social Engineering Attack Vectors 38
3.4 Gender, Cybersecurity and Fraud Studies 42
3.4.1 Demographic Attributes: Gender, Age, Education 42
3.4.2 Personality and Character Traits 43
3.4.3 National Culture 45
3.5 Agents: Gender Representation and Fraud 45
3.5.1 Gender Representation of Agents 46
3.5.2 Agent Issues Through the Gender Lens 46

3.5.3 Agent Fraud and Misappropriation 47
3.6 Grievance, Resolution Mechanisms 48
4 Organizations and Cybersecurity Professionals 50
4.1 Internal Fraud 50
4.2 Gender Representation Among Cybersecurity Professionals 51
5 Conclusions 53
6 Recommendations 54

Table of Exhibits

Exhibit 1: Table of Cybersecurity Issues and Frauds 9
Exhibit 2: Women's Phone Ownership and Access to and Privacy of their Data 11
Exhibit 3: Mobile ownership gender gap, low & middle-income countries by region 12
Exhibit 4: Handset type owned, percentage of population 14
Exhibit 5: Gender gaps in mobile phone ownership 15
Exhibit 6: Handset type distribution, share of population by gender 16
Exhibit 7: Important barriers to owning a mobile phone 21
Exhibit 8: Women's Literacy and Confidence Levels and their Cybersecurity Practices 22
Exhibit 9: Peer Knowledge Networks 24
Exhibit 10: Women's Cybersecurity Awareness and Confidence Using DFS 33
Exhibit 11: SIM Swap Fraud Using Vishing and Pretexting 37
Exhibit 12: COVID-19 Smishing Scams 40

Table of Acronyms

2FA	Two Factor Authentication
AML	Anti-Money Laundering
ATM	Automated Teller Machine
BOP	Bottom of the Pyramid
CFT	Countering the Financing of Terrorism
CICO	Cash In / Cash Out
CERT	Computer Emergency Response Team
CIRT	Computer or Cybersecurity Incident Response Team
CISA	Cybersecurity and Infrastructure Security Agency
CSIRT	Computer Security Incident Response Team
DFS	Digital Financial Services
DFSP	Digital Financial Services Provider
DRC	Democratic Republic of Congo
ICCID	Integrated Circuit Card ID
ICT	Information and Communication Technology
ISC2	International Information System Security Certification Consortium
ID	Identification
IT	Information Technology
IMEI	International Mobile Equipment Identity
ITU	International Telecommunications Union
KYC	Know Your Customer
LDC	Least Developed Countries
MENA	Middle East and North Africa
MFS	Mobile Financial Services
MNO	Mobile Network Operator
MMO	Mobile Money Operator
OTC	Over the Counter
PIN	Personal Information Number
PSA	Public Service Announcement
SIM	Subscriber Identity Module
SMS	Short Message Service
SSA	Sub-Saharan Africa
SA	South Asia
SSN	SIM Serial Number
STEM	Science, Technology, Engineering and Math
STK	SIM Toolkit
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organization
US	United States
USSD	Unstructured Supplementary Service Data

1 Overview

1.1 Introduction

Significant gender inequalities exist, especially pronounced in the developing world. Women consistently tend to lag behind men, to varying degrees, in access to information and communications technology (ICT), financial services, education, the marketplace, employment opportunities, and other rights and resources which may be based on social and cultural divides.[3]

The question presented in this paper is how issues related to gender, focusing primarily on unbanked and underserved women, may impact on customer vulnerability to fraud and of their cybersecurity behavior in the context of the Digital Financial Services (DFS).[4] DFS refers to a broad range of financial services that are accessed and delivered via digital channels, primarily mobile phones, and are intended to address the needs of the unbanked and underserved in developing countries.[5] It aspires to improve financial inclusion by shifting the provision of financial services from banks to non-banks. Accordingly, we sought to uncover information that would provide insight into the impact of the aforementioned issues on unbanked and underserved women, those at the bottom of the pyramid (BOP)[6] who reside predominantly in rural areas of developing countries.[7]

1.2 Scope and Methodology

The scope of this paper spans developing regions where DFS is most prominent and the largest perceived gender divides exist – those being Sub-Saharan Africa (SSA) and South Asia (SA), with occasional observations of the Middle East and North Africa (MENA). Cybersecurity and fraud issues relating to DFS in which a gender influence may be perceived are those issues which concern or target humans and their behavior rather than machines. The predominant issues are social engineering frauds, identity theft, monetary scams, cybersecurity awareness and hygiene.

---

[3] For more information about the basis of assumptions made relating to the population of this study, see Section 2.1 The Digital Gender Divide: Mobile Access, Handsets and Usage; See also Tiwari, JA and Srivastava, Bhavana, Chatterjee, R et. al. (2019) *Gender Centrality of Mobile Financial Services in Bangladesh*, available at https://bit.ly/3hQZ7XR.

[4] Fraud is generally defined as the actions of a bad actor intentionally making false representations so as to incur an unfair (usually financial) gain or cause loss to another. See Farooq, S (2019) *Mitigating common fraud risks: Best practices for the mobile money industry*, GSMA, available at https://bit.ly/3fLZm4m

[5] Perlman, L (2018) *DFS Primer*, available at www.dfsobservatory.com

[6] The term refers to the poorest but largest group of persons on a pyramid representing the global human wealth disparity and massive number of people living in poverty. Prahalad, CK and Hart, SL (2002) *The Fortune at the Bottom of the Pyramid*, available https://bit.ly/311V1G6; For the purposes of this paper, the BOP refers to such persons who are within developing countries in the region of study and also referred to as "global and national extreme poverty rates at the international poverty line of $1.90 a day per person, in 2011 purchasing power parity (PPP) terms." Fantom, N & Khokhar, T & Purdie, E (2016) *The 2016 edition of World Development Indicators is out: three features you won't want to miss*, available at https://bit.ly/386FAjs

[7] The term "developing countries" is defined as has been traditionally used by the World Bank and now referred to as "low- and middle-income" countries. Fantom, N & Khokhar, T & Purdie, E (2016)

This study began with an initial determination of the landscape, identifying the most common types of handsets used for DFS by women in the BOP in these regions, which was determined to be basic phones and feature phones with limited to no Internet access.[8] As covered in Section 1.4, there is a paucity of quantitative and qualitative data on cybersecurity and fraud in relation to DFS, especially gender disaggregated. Given this limitation, we used indirect data sources and published usage patterns of technology use to attempt to build a view of potential gender-related issues that may sway, if at all, fraud and cyber risk in relation to DFS access and use. This method represents efforts to aggregate relevant data to form a better appreciation and understanding of the role gender may play as it relates to vulnerability to fraud and cybersecurity in the context of the DFS environment. Much of the data which forms the basis of this paper covers SA, where gender inequalities relating to general access to resources earlier identified as being largest (such as ICT, financial services, education and the marketplace) and where efforts to bridge these gaps have been documented.

Section 1 presents introductory summaries of DFS and relevant cybersecurity and fraud issues which may be related to gender. Section 2 identifies digital divides and defines the mobile handset types which form the basis for this study. It also examines gender inequalities in developing nations which may provide insight into cybersecurity behavior and susceptibility to fraud in the context of the DFS environment. Section 3 follows with an examination of common DFS frauds and cybersecurity behavior which may be shaped and impacted by gender issues. Section 4 provides a brief summary of conclusions.

To facilitate with organization and ease of reading, technical granularity and additional background information has been placed within footnotes. We have used industry standard web address shorteners throughout this study to improve readability of the footnotes, with all URLs verified as of June 25, 2020. Research was undertaken through desktop research, interviews with practitioners, industry consultants and attendance at international conferences. Research was conducted from April through May 31, 2020.

The authors would like to thank the following people for their assistance with research for this paper: Anup Singh, Regional Head - Anglophone Africa, MSC (MicroSave Consulting); Akhand Jyoti Tiwari, Principal Consultant, MSC (MicroSave Consulting); Sunitha Rangaswami, Gender Equality and Women's Economic Empowerment Expert; Anna Collard, SVP of Content Strategy & Evangelist, KnowBe4 Africa; Laura Tich and Evelyn Kilel, Co-Founders, ShehacksKE; and Brencil G. Kaimba, Information Security Consultant, Serianu.

[8] For more information about the basis for the assumption made about the population of this study, see Section 2.1 The Digital Gender Divide: Mobile Access, Handsets and Usage;; See also Tiwari, JA and Srivastava, Bhavana, Chatterjee, R et. al. (2019) *Gender Centrality of Mobile Financial Services in Bangladesh*.

1.3 Introduction to Digital Financial Services (DFS)

Digital Financial Services[9] is intended to address the needs of the poor, unbanked and underserved in developing countries, aspiring to improve financial inclusion by shifting the provision of financial services from banks to non-banks. Access is provided predominantly through the use of low-cost mobile phones providing basic functionality which acts as a payment instrument utilizing a mobile money transfer system[10] where mobile wallets are linked to telephone numbers. Many of these services are offered by Mobile Network Operators (MNOs) and Digital Financial Service Providers (DFSPs).

A majority of the poorest members of the population reside predominantly in rural areas,[11] regions which feature limited mobile coverage and power availability.[12] Mobile infrastructure still makes it possible to overcome operational barriers in these areas and make financial services increasingly accessible and affordable to residents. Most frontline services, such as customer signup and cash-related services such as Cash-in and Cash-out (CICO)[13] operations, are performed by commissioned DFS 'agents' contracted to DFS providers who are situated in strategic locations across rural areas.[14] The DFS bouquet of products and services includes payments and remittances, savings, loans, investments, insurance among others.

[9] DFS is a broader system than mobile financial services (MFS). They are grouped under the umbrella of DFS terminology. See Tiwari, JA and Srivastava, Bhavana, Chatterjee, R et. al. (2019) *Gender Centrality of Mobile Financial Services in Bangladesh*; Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC, available at https://bit.ly/2YoQYCh.

[10] Mobile money transfer consists of "[s]ervices whereby customers use their mobile device to send and receive monetary value - or more simply put, to transfer money electronically from one person to another using a mobile phone." Firpo, J (2009) *E-Money – Mobile Money – Mobile Banking – What's the Difference?*, available at https://bit.ly/2YlJ50b

[11] Hernandez, E (2019) *Agent Networks at the Last Mile: A Guide for Digital Finance to Reach Rural Customers*, available at https://bit.ly/2Ynbi6S; Wechsler, M and Gurung, N and Perlman, L (2018) *The State of Regulatory Sandboxes in Developing Countries*, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3285938; The World Bank estimated that, in 2014, 70% of the population of Kenya lived in rural areas, making under $50 per month, with few employment opportunities which are primarily in agriculture. Wyche, S and Olson, J (2018) *Kenyan Women's Rural Realities, Mobile Internet Access, and "Africa Rising"*, available at https://bit.ly/3fPy119.

[12] Wechsler, M and Gurung, N and Perlman, L (2018) *The State of Regulatory Sandboxes in Developing Countries.*

[13] Cash-in is the process of converting cash into mobile money and cash-out is the conversion mobile money into cash, both using the DFS agent who is sometimes referred to as a "human ATM" (automated teller machine).

[14] Wright, G (2017) *The Clear Blue Water on the Other Side of the Digital Divide*, Microsave, available at https://bit.ly/2iXaJeo

1.4 Cybersecurity and Fraud in DFS with a Gender Lens

Cybersecurity Behavior and Fraud in DFS. Prior research has identified the primary types of cybersecurity[15] concerns related to DFS[16] along with risk factors and vulnerabilities related to DFS fraud.[17] The predominant types of cyber-attacks threatening financial inclusion *services providers* are data breaches and insider attacks, system outages and denial of service attacks and third-party threats; social engineering attacks and DFS scams.[18] With regard to consumers, who are the primary focus of this study, the growth of DFS been marked by a significant increase in consumer fraud.[19] Most notable are social engineering scams (examined in Section 3.3) and identity theft (examined in Section 3.3.1.2), which can result in substantial monetary damages and loss of mobile services to victims who can least afford them. A summary of the issues examined in this section are contained in a chart at the end of this introduction, in **Exhibit 1***, Table of Cybersecurity Issues and Frauds.*

The Gender Lens. Significant gender inequalities can exist in social, cultural, educational and economic conditions in developing countries. Data and interviews suggest that countries studied within SA (such as Pakistan and Bangladesh) may have more pronounced gender gaps with greater social and cultural gender roles than those in SSA (such as Kenya.) An overall comparative measure of gender disparity within SSA, MENA and SA was reviewed using the United Nations' Gender Inequality Index, which indicated that developing countries in this study were located primarily in the bottom tiers.[20] ICT and DFS access studies yielded consistent, substantial gender gaps primarily favoring men.[21] Taken as a whole, women at the BOP – especially in rural areas – appear to be consistently lagging behind men regarding the technology they use, their access to and use of DFS in being: notably less likely to own a mobile phone; less likely to own a smartphone; less likely to have or make use of Internet access; more likely to face literacy and numeracy challenges; less educated overall with less financial and technical literacy and, accordingly, less likely to have a DFS account.

---

[15] Cybersecurity is defined concisely as "[t]he state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this." Oxford University Press (2020) *Meaning of Cybersecurity*, available at https://www.lexico.com/definition/cybersecurity

[16] Primary cybersecurity concerns in DFS are system downtime, third party threats, internal fraud, data breaches and identity theft. Nduati, H (2018) *Cyber Security in Emerging Financial Markets*, available at https://bit.ly/2NhZxIv; Baur-Yazbeck, S (2018) *4 Cyber Attacks that Threaten Financial Inclusion*, available at https://bit.ly/2YP89M0; Buku, M and Mazer, R (2017) *Fraud in Mobile Financial Services: Protecting Consumers, Providers, and the System*, available at https://bit.ly/3dtH8Dv.

[17] MFS fraud risk factors and vulnerabilities include product; channel; agent; customer and compliance; system and delivery; and regulatory, supervisory and enforcement risks. Buku, M and Mazer, R (2017) *Fraud in Mobile Financial Services: Protecting Consumers, Providers, and the System*.

[18] Baur-Yazbeck, S (2018) *4 Cyber Attacks that Threaten Financial Inclusion*.

[19] Fraud is generally defined as the actions of a bad actor intentionally making false representations so as to incur an unfair (usually financial) gain or cause loss to another. See Farooq, S (2019) *Mitigating common fraud risks: Best practices for the mobile money industry*, GSMA.

[20] The United Nations Gender Inequality Index provides a relative global comparison measuring how women are disadvantaged in relation to three dimensions: reproductive health, empowerment and the labor market. Countries that are the study in this paper are found towards the bottom half beginning with Sri Lanka at 76, Algeria 85, Jordan 95, India 130, Bangladesh 136, Kenya 142, Pakistan 150, Nigeria 157 and Mozambique 180. UNDP (2020) *Table 5: Gender Inequality Index*, available at http://hdr.undp.org/en/composite/GII

[21] A list of study sources is contained in footnote 26.

Data Scarcity and Sources. Overall, gender disaggregated data is rare, especially within the smaller DFS universe,[22] and may not have been captured at time of collection.[23] A literature scan indicates that there is very little published data on gender differences relating to susceptibility of people to cybersecurity and fraud risks, generally, and specifically in relation to financial services. Where fraud data released by national computer emergency response teams (CERTs)[24] exists, they are often broad and lack sufficient quantitative and qualitative detail useful for analysis. Fraud information is generally not publicly disclosed by MNOs and DFSPs, probably for reputational purposes.[25]

Accordingly, data aggregation for constructing a gender lens, as shown in Section 2 below consisted of *inter alia*: identification, compilation and extraction of regional ICT and DFS gender disaggregated data resulting from a limited number of studies and surveys of developing countries by international organizations, global industry groups, regional think tanks and studies from local consulting firms;[26] a review of relevant DFS, social engineering and gender related studies; interviews from experts who have conducted ground work, providing additional context into cultural and socio-economic norms impacting on gender and DFS including reporting insights and confirming observations on how unbanked and underserved women approach cybersecurity and fraud issues in DFS.

[22] Interviews with practitioners, industry consultants, and field experts who explained that in various countries, such as India, financial institutions had but didn't disclose information collected regarding gender or it had been more recently required.
[23] Generally speaking, gender disaggregated data is scant, may not be collected at time of surveys and may be deprioritized if women are not perceived as being an important demographic by the marketplace and industry. Efforts are being made at collection in India with regard to "PMJD EK, SR, AT and AS in May 2020. See also Microsave (2019) *The real story of women's financial inclusion in India*, available at https://bit.ly/2Z46pPp.
[24] Detailed cybersecurity data is often not available from governmental sources, such as CERTS. Using the National Kenya Computer Incident Response Team – Coordination Centre (National KE-CIRT/CC) as an example, cyberthreat statistics are reported in broad categories such as malware, DDOS/Botnet, Web Application Attacks and System Vulnerabilities. Breakdown of statistics, such as social engineering attacks or details such as phishing and smishing are not reported. MNO incidents are reported in the aggregate without detail. National KE-CIRT/CC (2019) *First Quarter Sector Statistics Report for the Financial year 2019/2020*, available at https://bit.ly/3hQZGkr
[25] Fraud and grievance mechanism data from MNOs and DFSPs is generally not publicly available. Its opacity may be explained by the presence of high reputational risk and substantial reduction of consumer confidence in the DFS ecosystem. Interviews with practitioners, industry consultants, and field experts.
[26] Several relevant studies included in this paper were conducted by the World Bank, ITU, IFC, UN, GSMA, LIRNEasia and Research ICT Africa.

DFS Customers: Issues and Victim of Fraud by Customers/Third Parties			
Issue	**Type**	**Risk**	**Potential Gender Influences / Issues**
Attack Vectors (Social Engineering)	- Phishing - SMS Scams (smishing) - Voice Scams (vishing) - Impersonation	Fraud, identity & data theft, unauthorized access to and control over financial and other accounts	Lower literacy, numeracy & digital literacy. Possible lower cyber awareness and limited access to peer knowledge networks.
Fraud (money transfer)	Advance Fee, Extortion, Sympathy Purported Wrong Transfer scams	Loss of funds sent by consumer	Possible susceptibility to sympathy scams but risk aversion may limit money transfer susceptibility
Fraud (data access)	ID Fraud/Theft, PIN/Sensitive Information Disclosure	Fraud, identity & data theft, unauthorized access to connected accounts	Possible greater susceptibility to compliance scams
Fraud	SIM Swap	Loss of mobile service & connected assets	Possible susceptibility due to lack of technical literacy, cyber- awareness
Issue	Automatic Transactions	Limits fraud detection	Limited literacy limits awareness of potential issues
Issue	Shared Phone Access	Loss of funds, privacy	Women disadvantaged due to lack of phone ownership and exclusive control
Issue	ID/KYC Hurdles	Inability to obtain ID	Legal limitations in some jurisdictions
Issue	Sexual Harassment	Victimization/intimidation	Female victimization more likely
DFS Agents: Issues and Frauds			
Fraud	Split Deposit/Withdrawal	Fraudulent commissions	Lower literacy, numerosity
Fraud	Illegal customer charges, tips, fees	Customer loses extra charges from transaction	Lack of awareness
Fraud	Unauthorized PIN access	Loss of funds in transaction Exploitation of PIN by agent	Low literacy, numeracy creates agent dependency & susceptibility
Fraud	Unauthorized use of customer transaction code	Loss of funds from the "failed" transaction	More vulnerable due to lack of cyber awareness, knowledge networks
Organization: Issues and Frauds			
Fraud	Unintentional Internal Fraud, Data Breaches	Social Engineering attacks impacting MNOs/customers	Women may or may not be as vulnerable as men
Fraud	Internal Fraud (MNO, DFSP)	Employee fraud, theft and sale of sensitive information of customer and provider	Women may or may not be as vulnerable as men (mixed anecdotal opinions)
Issue	Grievance Redress Mechanisms (GRM)	Reputational risks, Under-reporting of fraud, Lower confidence in provider	Women are at a disadvantage due to male dominated GRM
Issue	Gender representation – too few women as cybersecurity professionals	Unbalanced gender teams may create unbalanced risks; minimized insight into women's issues.	Educational divide and traditional gender roles limit women in STEM fields compared to men

Exhibit 1: Table of Cybersecurity Issues and Frauds

This table represents a short summary of issues relating to consumers, agents and organizations

2 Gender Divides

Significant differences and inequalities exist across various planes such as between people in different regions, in developed and developing countries, in urban and rural areas, and between the genders of those who reside within them.[27] Women in developing countries can experience notably higher levels of inequality compared to men and may experience varying degrees of marginalization and discrimination resulting in more limited opportunities for capacity building and economic and social mobility. This can profoundly affect women's exposure to ICT and DFS, the manner in which they approach, understand and use technology and DFS, and their general levels of awareness of that which may be impacting within the realm of cybersecurity and digital fraud issues they may encounter.[28] This Section 2 summarizes relevant gender inequalities and divides.

2.1 The Digital Gender Divide: Mobile Access, Handsets and Usage

This section examines gender gaps relevant to the digital divide, a term often used to describe a comparative level of inequality relating to access to and the quality of ICT.[29] Our study is limited to a broad overview of developing countries in Africa and South Asia where meaningful gender disaggregated data has been reported. This section begins with a determination of what types of mobile handsets are likely to be predominantly in use by and potentially owned by women in these regions, whether gender gaps exist and to what extent.

Our review concludes that while smartphones are becoming more popular – especially in urban areas – they are still primarily an outlier in rural areas where most of the BOP reside. Reports indicate that women are still more likely to use predominantly basic and feature phones without mobile Internet access.[30]

2.1.1 Mobile Coverage and Mobile Internet Access

As of 2018, an estimated 40% of the population living in Sub-Saharan Africa (SSA) are outside of mobile coverage footprints with the lowest global Internet penetration in SSA (24%), South Asia (SA) (33%) and the Middle East and North Africa (MENA) (40%).[31] These regions also exhibited the lowest proportions of women using the mobile internet (SSA 29%, SA 27%, MENA 44%) and also the most pronounced gender gaps in comparison to men for use (SSA 41%, SA 58%, MENA 20%).[32] These numbers suggest

[27] Most studies in this paper do not define gender other than comprising of male and female. This paper does not distinguish these studies from those which explicitly recognize, distinguish and study gender identification and transgender persons. For example, see Sambasivan, N and Batool, A and Ahmed, N et. al. (2019) *"They Don't Leave Us Alone Anywhere We Go": Gender and Digital Abuse in South Asia*, available at https://bit.ly/2CopPqh.
[28] UN (2020) *Inequality – Bridging the Divide*, available at https://www.un.org/en/un75/inequality-bridging-divide
[29] Hilbert, M (2011) *The end justifies the definition: The manifold outlooks on the digital divide and their practical usefulness for policy-making. Telecommunications Policy*, available at http://dx.doi.org/10.1016/j.telpol.2011.06.012
[30] In developing countries, smartphones are often not near the quality levels found in many developed countries, often low-cost, low-quality imports. Even when new, they can suffer from poor build quality, inferior components, low resolution and low responsive screen and poor battery life. Wyche, S and Olson, J (2018) *Kenyan Women's Rural Realities, Mobile Internet Access, and "Africa Rising*; Interviews with practitioners, industry consultants, and field experts.
[31] Bahia, K and Suardi, S (2019) The *State of Mobile Internet Connectivity*, GSMA, available at https://bit.ly/3hLjoOm.
[32] Bahia, K and Suardi, S (2019) The *State of Mobile Internet Connectivity*, GSMA.

that a substantial percentage of women in these regions do not use the Internet and, where they do and which is predominantly in urban areas, their usage rates still lag meaningfully behind men.

2.1.2 Ownership and Sharing

Mobile Phone Ownership. Empowerment provided by phone ownership can play a substantial role in appreciating gender issues. A significant number of unbanked women – especially in countries where there is a history of patriarchal and conservative social, religious and cultural norms which can manifest in more pronounced gender divides such as Bangladesh, Pakistan and India – do not have access to a mobile.

When women do have access to mobile phones, they may not own the device and access may be provided primarily through shared household phones or those borrowed from other family members, predominantly males.[33] Mobile phone priority in local culture often begins with the breadwinner who leaves the home for work, which also tends to be male, although the phone may be communally available to the household, as is the case in Myanmar.[34] As additional phones are purchased and upgraded, new and enhanced handsets (such as smartphones) usually fall within similar order of priority. More information about the relationship of women's phone ownership and sharing is discussed in **Exhibit 2**.

Phone ownership can encourage women to become more invested in technology and DFS, gaining knowledge, experience and confidence through use. But over 74 million females in SSA and 207 million more in South Asia still do not own a mobile phone with a 13-23% gender gap still existing across these regions.[35] Social, cultural and religious factors can play a role in women's limited comfort and autonomy with mobile devices. Unbanked and underserved women have been traditionally been less likely to be able to select and purchase a handset, top up for airtime and have exclusive control over their phone including data usage privacy. Men tend to fear that their sisters or wives may be harassed, abused or led astray by other men through digital means.[36] Accordingly, shared phones represent a significant challenge in a woman's ability to secure their data, maintain their privacy, knowledge about their finances, and be empowered as independent users of DFS.

Exhibit 2: Women's Phone Ownership and Access to and Privacy of their Data
Women own fewer mobile phones than men, share more frequently.

[33] Zainudeen, A and Galpaya, H (2015) *Mobile phones, internet, and gender in Myanmar*, available at https://bit.ly/3emDJrl; Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh*, IFC.
[34] Zainudeen, A and Galpaya, H (2015) *Mobile phones, internet, and gender in Myanmar*.
[35] The gender gap refers to how much less likely a woman is to use mobile internet than a man. GSMA (2020*) The Mobile Gender Gap Report 2020*, available at https://bit.ly/2ZaJMZJ
[36] GSMA and Altai Consulting (2015) *Bridging the gender gap: Mobile access and usage in low- and middle-income countries*; Interviews with practitioners, industry consultants, and field experts.

Mobile phone borrowers are more likely to be women, as illustrated in several developing countries in SSA and SA.[37] A 2018 IFC study of women in rural areas of Bangladesh (IFC Bangladesh Study)[38] indicated that a majority of women owned mobile phones (68%) but a high degree of phone sharing also existed (28%), usually as a communal family phone or with another family member. Only 16% had access to smartphones.[39] Phone sharing is more common among adults with lower income and education levels, such as in India, where a Pew Research survey indicated that 17% of lower income individuals shared phones, with a sizable 15% gender gap (20% female to 5% male.)[40]

In SSA, women are 13% less likely than men to own a mobile phone and 41% less likely to use the mobile Internet.[41] (See **Exhibit 3**: Mobile ownership gender gap, low & middle-income countries by region.) The issue of sharing, which presents cybersecurity and privacy problems due to exposure of personal data to multiple persons, appears less pronounced in SSA than in SA.

Region	Gender Gap	Mobile Ownership Rate for Women	Women Unconnected
LATAM	1%	86%	30m
MENA	9%	82%	23m
Europe & Central Asia	-1%	92%	14m
Sub-Saharan Africa	13%	74%	74m
South Asia	23%	65%	207m
East Asia & Pacific	1%	95%	44m
Overall	8%	82%	393m

Exhibit 3: Mobile ownership gender gap, low & middle-income countries by region

The gender gap refers to how less likely a woman is to own a mobile than a man. **Mobile ownership** is defined as having sole or main use of a SIM card (or a mobile phone that does not require a SIM), and using it at least once a month. Based on survey results and modeled data for adults aged 18+. *Source: GSMA Intelligence, 2019.*[42]

[37] A 2016 GSMA report consistently indicating higher levels of female sharing such India (29%), Niger (19%), Indonesia (10%), Kenya (7%) and the DRC (6%). GSMA and Altai Consulting (2015) *Bridging the gender gap: Mobile access and usage in low- and middle-income countries*, available at https://bit.ly/3emqG9j

[38] Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh*, IFC.

[39] Tiwari, JA and Srivastava, Bhavana, Chatterjee, R et. al. (2019) *Gender Centrality of Mobile Financial Services in Bangladesh*; Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC.

[40] Sharing tends to be more common among adults with less education and lower income levels and impacts on their technical literacy levels. Silver, L and Vogels, E and Mordecai, M et. al. (2019) *Phone sharers: What limits their mobile use?*, available at https://pewrsr.ch/2YUpWl3

[41] Bahia, K and Suardi, S (2019) The *State of Mobile Internet Connectivity*, GSMA.

[42] GSMA (2020) The Mobile Gender Gap Report 2020,

A 2019 GSMA report indicated smartphone penetration of 39% in SSA, 49% in SA and 51% in MENA, making no distinction between country and area classification.[43] A breakdown of seven countries in Africa and SA indicated six still having greater basic and feature phone ownership. Surveys conducted in 2017 by LIRNEasia and Research ICT Africa (AfterAccess Study)[44] were consistent, indicating a majority of basic and feature phone ownership in 12 of 13 surveyed jurisdictions in Africa and SA, as appears in **Exhibit 4**.[45]

Overall, ownership of "basic" phones is most common overall in SSA, MENA and SA with a notable representation of "feature" phones in select countries, such as India. Operational, resource and coverage limitations in rural areas may explain the continued popularity of resource efficient basic and feature phones[46] with text-based interfaces, using Unstructured Supplementary Service Data (USSD)[47] and SIM Application Toolkit (STK)[48] for DFS. The AfterAccess Study[49] also reported gaps of lower ownership levels in rural areas, where a majority of the unbanked and underserved reside,[50] consistently indicated throughout SA and Africa.

[43] These percentages reflect the inclusion of developed countries and urban areas and are likely to be substantially lower in developed countries and within rural areas. Bahia, K and Suardi, S (2019) The *State of Mobile Internet Connectivity*, GSMA.
[44] These surveys were conducted in a joint effort by a joint effort DIRSI, LIRNEasia and Research ICT Africa. LIRNEasia (2020) *AfterAccess Archives – LIRNEasia*, available at https://lirneasia.net/after-access
[45] The highest levels of basic and feature phone ownership appeared in India, Pakistan, Bangladesh, Senegal, Kenya, Tanzania, Rwanda, Uganda and Mozambique. Only Nepal indicated a small 4% difference in favor of smartphone ownership. AfterAccess, LIRNEasia (2019) *ICT access and use in Asia and the Global South*, available at https://lirneasia.net/2019/05/afteraccess-asia-report3/
[46] A substantial lack of reliable mobile broadband coverage and power charging options significantly limits the utility of smartphones in rural areas. Perlman, L and Wechsler, M (2018) Mobile Coverage and its Impact on Digital Financial Services, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=337066
[47] Unstructured Supplementary Service Data (USSD) is a novel standard within the GSM and 3G specifications, seen both as a narrowband data transmission mechanism and user interface. Perlman, L and Wechsler, M (2018) Mobile Coverage and its Impact on Digital Financial Services.
[48] SIM Toolkit (STK) is a popular encrypted SMS-based remote access and UI GSM technology used to provide DFS and related services to markets where basic and feature phones are the plurality. Perlman, L and Wechsler, M (2018) Mobile Coverage and its Impact on Digital Financial Services.
[49] AfterAccess, LIRNEasia (2019) *ICT access and use in Asia and the Global South*.
[50] For more information, see Footnote 11.

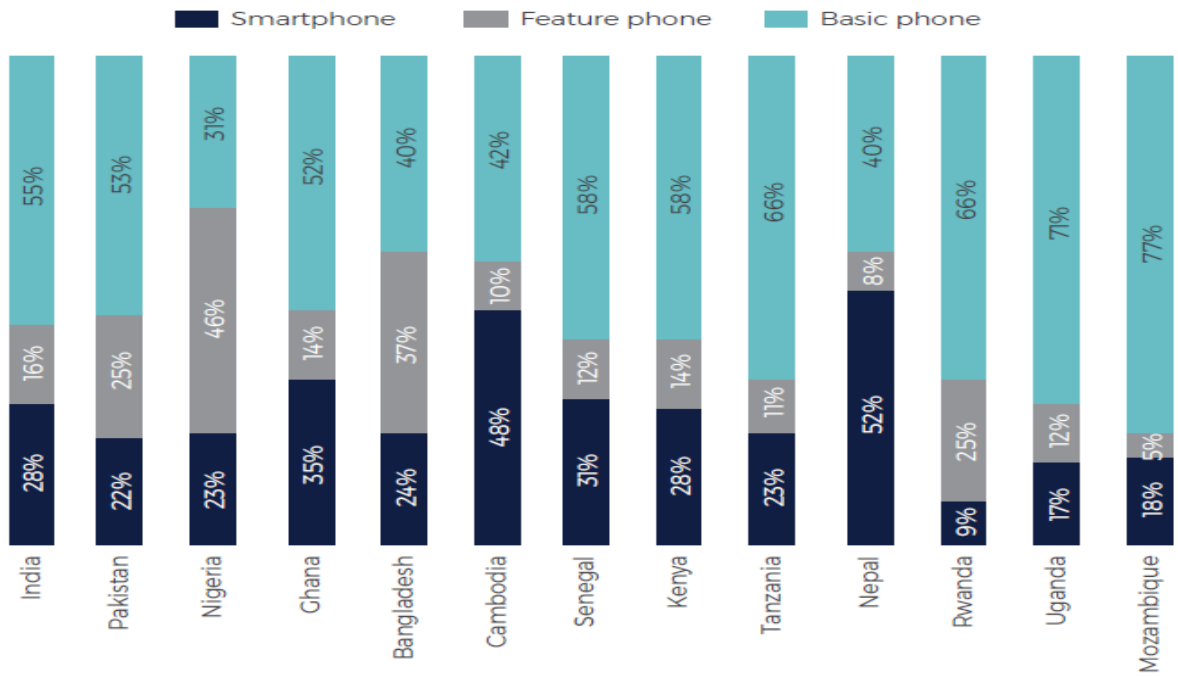

Exhibit 4: Handset type owned, percentage of population
Respondents are categorized according to their most advanced device owned, and can only be included in one category. Smartphone owners that also own a basic or feature phone are counted only as smartphone owners. Device owners included only if they have an active SIM, or a mobile phone that functions without a SIM. *Source: LIRNEasia, 2019.*[51]

Gender Gaps in Mobile Phone Ownership. Regionally, the GSMA reported the largest gender gaps in mobile phone ownership, consistently favoring males, in SA (23%) and SSA (13%). The AfterAccess Study indicates the largest ownership gender gaps (all favoring males) in South Asia – India (46%), Pakistan (34%), Bangladesh (34%) – and smaller but still sizable gaps in Africa in Mozambique (27%), Uganda (29%) and Nigeria (18%), as appears in **Exhibit 5**.

[51] Results reflect a study of DIRSI, LIRNEasia, Research ICT Africa (2019) *AfterAccess ICT access and use in Asia and the global south version 3.0 April 2019*, available at https://lirneasia.net/2019/05/afteraccess-asia-report3/

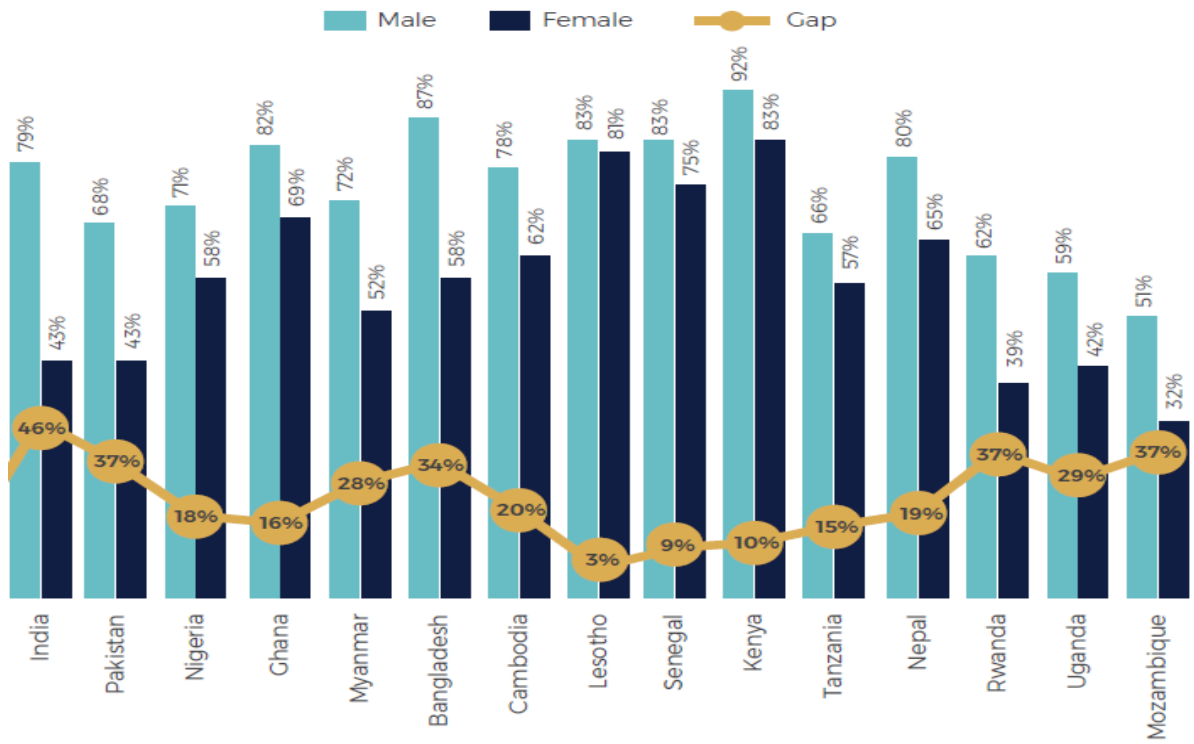

Exhibit 5: Gender gaps in mobile phone ownership
Respondents are categorized according to their most advanced device owned, and can only be included in one category. Smartphone owners that also own a basic or feature phone are counted only as smartphone owners. Device owners included only if they have an active SIM, or a mobile phone that functions without a SIM. (Percentage of the population aged 15-65.) *Source: LIRNEasia, 2019.*[52]

Gender Gaps in Handset Types. As per Exhibit 6, the GSMA found consistently large gender gaps for smartphone ownership, significantly favoring men, across seven surveyed African and South Asian countries. The most pronounced gender gaps indicating women's ownership of basic phones exceeding men's ownership were in countries also having the largest gaps favoring men as smartphone owners (Algeria, Nigeria, India.)[53]

[52] DIRSI, LIRNEasia, Research ICT Africa (2019) *AfterAccess ICT access and use in Asia and the global south version 3.0 April 2019*, available at https://lirneasia.net/2019/05/afteraccess-asia-report3/
[53] Note a distinction between studies: the GSMA survey skews data in favor of smartphone ownership, more common in urban areas, by counting phone ownership once using the highest level of technology available to the user.

This is consistent with the earlier observation that males typically own or upgrade to smartphones before women[54] along with data indicating that there is less disparity among the youth, who are also more likely to own smartphones and moving overall towards smartphone adoption.[55]

Feature phones still have a notably large footprint in Tunisia and India.[56] It is still important to note that, in the context of developing nations, the concept of "smartphones" can be easily distinguished from the standard issue in many developed countries in being low-end devices with subpar battery life, screen quality and digitizer, resolution and overall manufacturing quality.[57]

	Smart		Feature		Basic	
Country	**Men**	**Women**	**Men**	**Women**	**Men**	**Women**
Algeria	68%	55%	2%	2%	20%	26%
Mozambique	22%	18%	6%	4%	27%	24%
Nigeria	48%	39%	16%	15%	24%	27%
Uganda	19%	13%	27%	20%	34%	32%
Bangladesh	36%	21%	31%	26%	19%	13%
India	37%	14%	9%	6%	29%	31%
Pakistan	37%	20%	7%	6%	39%	23%

Exhibit 6: Handset type distribution, share of population by gender
Respondents are categorized according to their most advanced device owned, and can only be included in one category. Smartphone owners that also own a basic or feature phone are counted only as smartphone owners. Device owners included only if they have an active SIM, or a mobile phone that functions without a SIM. *Source: GSMA Intelligence, 2018*.[58]

Mobile Device and Usage Assumption. As the data suggests that a majority of persons overall in Africa and SA still appear to be using basic and feature phones, a presumption may be made that the subset of female DFS users do so at the same or more pronounced levels as would be consistent with earlier data related to gender gaps in mobile phone ownership.

[54] See Section 2.1.2 Phone Ownership and Sharing.
[55] Silver, L (2019) *Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally*, available at https://tinyurl.com/y4vu5wkf; Interviews with practitioners, industry consultants, and field experts. See also GSMA growth tracking and estimates. GSMA (2020) *The Mobile Economy 2020*, available at https://bit.ly/37PEDtK.
[56] Smartphone ownership is overall and may not significantly reflect the representation of ownership by the BOP in rural areas. Research indicates that while Kenya and India have 36% and 32% smartphone ownership among adults, basic phone ownership far exceeds these numbers with 40% and 47% respectively. Silver, L and Smith, A and Johnson, C et. al. (2019) *Use of smartphones and social media is common across most emerging economies*, available at https://pewrsr.ch/2Ngr8d1.
[57] Wyche, S and Olson, J (2018) *Kenyan Women's Rural Realities, Mobile Internet Access, and "Africa Rising"*; Interviews with practitioners, industry consultants, and field experts.
[58] Bahia, K and Suardi, S (2019) The *State of Mobile Internet Connectivity*, GSMA.

2.2 DFS Onboarding, Account Ownership and Literacy Levels

As iterated above and within this Section 2, in developing countries, males are often head of household, in charge of finances and first in priority for ICT access.[59] Women have notably lower language literacy levels, economic opportunities[60] and DFS account ownership levels than men, in addition to unique onboarding hurdles in some jurisdictions. These barriers can reduce incentive in women to build DFS-related knowledge, capacity and comfort with technology which potentially reduces awareness of and increases vulnerability to cybersecurity risks and fraud. This section explores these divides which can also curtail financial inclusion.

2.2.1 DFS Onboarding

Implementation of digital national identification has been emerging as an important initiative for accessing DFS and other essential services, such as Aadhaar in India,[61] and Huduma Namba[62] in Kenya.[63] The 2017 Global Findex data found that the most prevalent use of an identification card was to apply for a subscriber identity module (SIM) card and MNO onboarding.[64] But women face a disproportionately more difficult burden in obtaining official identification (ID), especially in parts of South Asia and in more conservative rural areas where necessary documentation is difficult to obtain.

While possession of a verified identity is relatively high among unbanked adults,[65] the Global Findex data indicates an average of 8% fewer women own a national identity card across SSA, with sizable double-digit gender gaps in Afghanistan (46%), Pakistan (14%), Ethiopia (20%) and Mozambique (14%).[66] The World Bank's ID4D-Findex study reported that the difference in ID ownership between men and women exceeds 20 percentage points in Chad, Niger, Benin and South Sudan.[67] Legal and regulatory hurdles in

[59] See specifically Section 2.1 The Digital Gender Divide: Mobile Access, Handsets and Usage.
[60] See Section 2.3.1 Social, Cultural and Economic Divide.
[61] An Aadhaar number is a 12-digit random number issued by the Unique Identification Authority of India (UIDAI) to verified residents of India (2020) *What is Aadhaar*, available at https://uidai.gov.in/what-is-aadhaar.html
[62] Huuduma Namba (National Integrated Identity Management System (NIIMS) is Kenya's national identity system. In theory, the unique identifier can help address identity fraud. Republic of Kenya (2020) FAQs – What is Huduma Namba, available at http://www.hudumanamba.go.ke/faqs/; Republic of Kenya (2020) *The Registration of Persons (National Integrated Identity Management System) Regulations, 2020*, available at https://bit.ly/315pKSD.
[63] Huduma centers are one stop shop citizen centers where many popular departments of government are represented, e.g. transportation, immigration and identification for travel cards, passports, etc. The system, which features several hundred use cases, is an end to end digitized system with the ability to obtain physical documents at local centers which are dispersed in various Kenyan localities. See Huduma Kenya (2020) *Huduma Kenya*, at https://www.hudumakenya.go.ke/
[64] Demirguc-Kunt, A and Klapper, L and Singer, D et. al. (2017) *The Global Findex Database 2017, World Bank*, available at https://globalfindex.worldbank.org/
[65] Klapper, L and Hess, J (2019) *New Findex notes showcase digital financial inclusion in Sub-Saharan Africa*, available at https://bit.ly/3hOmdhF; Theodorou, Y and Okong'o, K and Yongo, E (2019) *Access to Mobile Services and Proof of Identity 2019: Assessing the impact on digital and financial inclusion*, available at https://bit.ly/313xjJz
[66] Demirguc-Kunt, A and Klapper, L and Singer, D et. al. (2017) *The Global Findex Database 2017, World Bank*; Theodorou, Y and Okong'o, K and Yongo, E (2019) *Access to Mobile Services and Proof of Identity 2019: Assessing the impact on digital and financial inclusion*.
[67] Close to 40% of adults in low-income countries (LICs) do not have an ID. Less-educated people, younger adults, people out of the workforce, and those living in rural areas, are also less likely to have an ID. Many people without an ID find it too

Cameroon, Chad, Gabon, and Niger make the process of opening a bank account more challenging specifically for women,[68] as is the case in other areas such as Bangladesh due to substantial social and cultural gaps.[69]

Women in Bangladesh can generally be hesitant to provide personal information and documentation to agents, especially in rural areas, for fear that men may copy and distribute documents and information which can create the potential for harassment.[70] In addition to the extended time needed for initial account setup (3-5 days), know-your-customer (KYC) regulations[71] require the submission of a photograph with a DFS application, which can present compliance challenges for women due to social, cultural and legal barriers in conservative and religious jurisdictions. Evading regulation is sometimes accomplished using a male relative for account setup, which will be used for female but also makes her dependent on the male relative.[72] This also prevents the female phone user from receiving cybersecurity and fraud awareness training that may be provided during onboarding.[73]

2.2.2 Financial Literacy and Account Ownership

Worldwide, women comprise of a noticeably larger portion of unbanked persons, which is generally consistent in most economies.[74] The 2017 Global Findex reported substantial gender gaps favoring men's ownership of a financial account in the SSA, MENA and SA regions. Well over 20 countries reported double digit gender gaps in account ownership with Jordan (29%), Bangladesh (29%) and Pakistan (28%) topping the list. Among those without a financial account, 14 countries had double digit gender gaps led by Morocco (15%), Bangladesh (15%) and Algeria (13%). In Africa, Nigeria and Mozambique had substantial double-digit gender gaps in both categories. Only 43% of adults had a financial account and 58% of women owned a mobile phone compared to 71% of men.[75]

---

difficult to obtain one. In countries with large ID coverage gaps (exceeding 20%), 1 in 3 adults without an ID find it "too difficult to apply"; not being able to provide supporting documents is also cited by many as a challenge. World Bank (2017) *Global ID Coverage, Barriers, and Use by the Numbers: Insights from the ID4D-Findex Survey*, available at https://bit.ly/38PV9uo

[68] Bill & Melinda Gates Foundation (2019) *Women's Digital Financial Inclusion in Africa*, available at https://gates.ly/31aMWyS ; Change has occurred but, as of 2014, the World Bank reported that nine countries had different rules for women to obtain national ID cards, 19 for obtaining passports and 29 being head of household. World Bank (2013) *Women, Business and the Law 2014*, available at https://bit.ly/2V2yk0D.

[69] Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC; Bangladesh Bank (2018) *Women Mobile Financial Services Agent Recruitment Manual 2018,* Bangladesh Bank (2018) *Women Mobile Financial Services Agent Recruitment Manual 2018*, available at https://www.bb.org.bd/fnansys/paymentsys/paysystems.php.

[70] Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market* See also Section 2.3.2 Gender Imbalances, Women's Confidence and Sexual Harassment.

[71] KYC procedures are regulatory compliant processes for verifying the identity of the customer – that the applicant is the actually the person they represent themselves to be.

[72] Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh*, IFC.

[73] At present, cybersecurity and fraud training is limited during onboarding, primarily focusing on upsell of DFSP products and services. For more information, see Section 2.2.4 Technical Literacy.

[74] Demirguc-Kunt, A and Klapper, L and Singer, D et. al. (2017) *The Global Findex Database 2017, World Bank.*

[75] Wintour, P (2019) *Melinda Gates pushes G7 to close digital gender gap in Africa*, The Guardian, available at https://bit.ly/2V5WTKc

Lower DFS account ownership numbers among women can stem from several factors in developing countries, especially those with strong conservative, religious and patriarchal influences, such as: traditional gender roles where males are expected to have greater financial literacy[76] and are in control of household finances; lower women's literacy and numeracy levels which makes use of DFS challenging; and the propensity to default to over-the-counter (OTC) transactions[77] if readily available – where transactions are conveniently offloaded to agents using their own accounts to conduct transfers on behalf of women without DFS accounts.[78]

As per the IFC Bangladesh Study, where OTC is prevalent, women may be resistant to graduate from basic necessities to other DFS products. Women in Bangladesh used DFS predominantly to receive money (94%) and send money (78%) using few other DFS products.[79] Only 20% were aware of fees and costs of DFS services and only 10% were aware of their rights as customers, making them optimal targets for agent fee frauds covered in Section 3.5.

The IFC Bangladesh Study, consisting of women, reported that only 4% of respondents received formal financial literacy training. The source of women's financial information came predominantly from household members (83%) with much smaller amounts originating from DFS agents (25%), friends (18%) and neighbors (16%). Women who have a more primitive understanding of technology and DFS and rely on others to conduct OTC transactions on their behalf are usually less aware of cybersecurity practices and more vulnerable to DFS frauds.[80]

2.2.3 Education, Literacy and Numeracy

Women's lower literacy and numeracy levels present barriers to women's DFS adoption and mobile Internet usage.[81] Overall, women's literacy rates are substantial lower than global averages in SSA (64.6%), and Central and South Asia (72.8%), with a low gender parity of 0.8 for adult women.[82] In Kenya where the national literacy rate is high at 79%, mean years of schooling are only 5.7 years for girls versus

[76] Interviews with practitioners, industry consultants, and field experts. Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC; Bangladesh Bank (2018) *Women Mobile Financial Services Agent Recruitment Manual 2018,* Bangladesh Bank (2018) *Women Mobile Financial Services Agent Recruitment Manual 2018*. See also **Exhibit 8.**

[77] For more information about OTC transactions, see Section 3.5.3 Agent Fraud and Misappropriation.

[78] Bangladesh Bank (2018) *Women Mobile Financial Services Agent Recruitment Manual 2018.*

[79] Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh*, IFC.

[80] Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC; Bangladesh Bank (2018) *Women Mobile Financial Services Agent Recruitment Manual 2018.* See also Section 3.2 Cybersecurity Issues, Awareness and Practices.

[81] GSMA (2020*) The Mobile Gender Gap Report 2020*.

[82] In the "Youth and adult literacy indicators 2017" table in its 2019 Global education monitoring report, UNESCO indicates the gender parity index or ratio of males to females attending school such that the .79 and .8 scores of SSA and SA translate to roughly 8 females for every 10 males. However, youth gender equality scores are approaching equality in these regions. UNESCO (2019) *Global education monitoring report 2019: Migration, displacement and education: building bridges, not walls*, available at https://unesdoc.unesco.org/ark:/48223/pf0000265866

7.1 years for boys.[83] Moving towards adulthood, a United Nations (UN) study of women's levels of educational participation revealed that women in SSA and SA were well below gender parity levels for primary educational levels, with a substantial drop in upper secondary education.[84]

Societal and cultural gender norms can set different expectations between men and women and shape expected social attitudes, behavior and roles.[85] Conservative and some religious environments with patriarchal gender norms can emphasize the role of women primarily as child bearers and household custodians rather than breadwinners, which can place less emphasis on their access to education and reduce their social mobility.[86] Women tend to marry at comparably younger ages in countries in SSA, MENA and SA and may dropping out of school to take care of family.[87]

This leads to low literacy and numeracy rates for women, leading them to having a high reliance on orality,[88] which creates additional challenges to use and understand technology and financial transactions. DFS transaction errors are among the most common reasons for monetary loss in DFS. The familiarity of women with such disappointment suggests that they might be more sympathetic to others with the same issue, possibly increasing their susceptibility to transaction reversal fraud.[89]

Traditionally, women in Kenya have been steered away from study and occupations involving science, technology, engineering and math (STEM) and towards social sciences and "women's jobs" such as general marketplace opportunities and agriculture.[90] While initiatives have been in place to increase participation in STEM studies and cybersecurity opportunities, cultural and social barriers still impact on young women, including challenges to be accepted into and study at secondary education levels which focus on cybersecurity and STEM subjects.[91]

[83] Research ICT Africa (2019) *After Access: The State of ICT in Kenya.*
[84] Compiled from the table "Women's level of educational participation, 2000-2017" in the cited 2019 UNESCO report. UNESCO (2019) *Global education monitoring report 2019: gender report: Building bridges for gender equality*, available at https://unesdoc.unesco.org/ark:/48223/pf0000368753
[85] Societal, cultural and religious factors including economic divides are examined in Section 2.3.
[86] Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh*, IFC.
[87] World Bank data reports that the average age women first marry in Bangladesh, India and Pakistan is below 20 years of age with African countries such as Mozambique, Kenya, Nigeria and Uganda ranging from below to early 20s. World Bank (2020) *Median Age At First Marriage (Women Ages 25-49): Q3*, available at https://bit.ly/31aN2qe; Kopf, D (2020) *The ages that people get married around the world*, available at https://bit.ly/2YmUCMX; Additional information pursuant to interviews with practitioners, industry consultants, and field experts.
[88] Hudson Matthews, Brett (2010) *Orality and Microsavings*, available at https://bit.ly/3140hcz.
[89] See Section 3.3.1.1 Theft of Funds.
[90] Interviews with practitioners, industry consultants, and field experts.
[91] Obira, M (2020) *Concerns raised on girls' dismal performance in STEM subjects*, available at https://bit.ly/3fLONhT; Interviews with practitioners, industry consultants, and field experts.

2.2.4 Technical Literacy

Women's financial and technical literacy levels also consistently lag below men's in developing countries in Africa and SA. Males are significantly more often heads of household and often in charge of finances, mobile phones and DFS accounts.[92]

GSMA surveys (appearing in Exhibit 7) found that low language and technical literacy skills were among the top barriers to owning a mobile phone by non-phone owners,[93] with low awareness of an understanding of the Internet in Africa and Asia.[94] Also observed was that women possess lower mobile technical literacy levels than men since they also trail with (i) lower levels of mobile phone ownership; (ii) lower literacy and educational levels (reading and writing, especially in Sub-Saharan Africa); and (iii) lower confidence levels in their ability to operate the phone.

	Don't know how to use a phone		Reading/Writing difficulties		Strangers contacting me		Family does not approve	
Country	**Men**	**Women**	**Men**	**Women**	**Men**	**Women**	**Men**	**Women**
Algeria	22%	27%	21%	30%	5%	5%	3%	21%
Kenya	0%	7%	15%	26%	6%	5%	0%	3%
Mozambique	6%	24%	16%	28%	2%	6%	2%	9%
Nigeria	9%	16%	45%	49%	4%	6%	6%	22%
Senegal	7%	7%	28%	30%	6%	18%	6%	4%
South Africa	3%	10%	10%	16%	0%	12%	3%	6%
Uganda	12%	15%	23%	21%	3%	4%	4%	10%
Bangladesh	19%	31%	46%	21%	0%	1%	6%	11%
India	11%	16%	18%	24%	12%	7%	3%	9%
Indonesia	21%	27%	36%	32%	4%	11%	1%	7%
Myanmar	40%	43%	22%	20%	13%	12%	2%	9%
Pakistan	10%	13%	56%	38%	5%	13%	7%	38%

Exhibit 7: Important barriers to owning a mobile phone

Percentage of non-mobile owners who identified the following as the single most important barrier to owning a mobile. 2019 Base: Non-mobile owners aged 18+ Mobile ownership is defined as a person having sole or main use of a SIM card (or a mobile phone that does not require a SIM), and using it at least once a month. See footnote for details. *Source: GSMA Intelligence Consumer Survey, 2019*.[95]

[92] Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh*, IFC.; Interviews with practitioners, industry consultants, and field experts.
[93] GSMA (2020*) The Mobile Gender Gap Report 2020.*
[94] AfterAccess, LIRNEasia (2019) *ICT access and use in Asia and the Global South*.
[95] From the GSMA report: "Percentages indicate the proportion of non-mobile owners who responded, "This is one of the most important reasons stopping me" to the question, "Which, if any, of those factors would you say are the most important reasons stopping you from having a mobile phone or SIM card, connected to a mobile operator's network?"" GSMA (2020) *The Mobile Gender Gap Report 2020*.

Consistent with these observations were the results from the IFC Bangladesh Study, which indicated that only 10% of women surveyed knew how to change their personal information numbers (PINs).[96] Women tended to rely on agents to provided them with transaction assistance, which included the sharing of PIN codes and assistance with changing them.[97] (See **Exhibit 8** regarding Women's Literacy Levels.)

When onboarding, technical assistance with mobile phones and DFS accounts is provided by agents. However, focus is often more concentrated on the sale and introduction of products of services with little in the way of educating the customer on cybersecurity practices beyond basic PIN management information.[98] At the time of initial contact, finding the optimal balance of convincing financial technology neophytes to trust the system while educating them on the potential dangers is a challenging process.

Women at the BOP are generally more averse to using technology. The presence of lower written and digital literacy rates results in words and digital interfaces being more difficult to comprehend and they are prone to making mistakes. Confidence levels are low and incentive to learn may also be limited where women do not perceive the added value or necessity of having a mobile phone. As such, these women may often rely on others for assistance, such as DFS agents, their husbands or other male figures in the household. In Pakistan, women tend to believe that their male family members are generally more knowledgeable about digital technology and financial issues and help the female members of the household with education and problem resolution.[99] This reliance on others makes women more vulnerable to cybersecurity and fraud.[100] Other examples include the MicroSave study of an Indian factory appearing in Exhibit 10 in section 3.2.

Exhibit 8: Women's Literacy and Confidence Levels and their Cybersecurity Practices
Unbanked women tend to have lower confidence levels with DFS and, even with moderate levels of education, may displace good cybersecurity practices in favor of assistance from others.

[96] "A personal identification number (PIN) code that is an authentication measure required for entry into a device or account. Most mobile money accounts require PIN codes for verification to prevent fraud." GSMA (2015) *Landscape Report: Mobile Money, Humanitarian Cash Transfers and Displaced Populations*, available at https://bit.ly/3fM365U.
[97] Interviews with practitioners, industry consultants, and field experts. See also **Exhibit 8.** Regarding Bangladesh, see Bangladesh Bank (2018) *Women Mobile Financial Services Agent Recruitment Manual 2018.*
[98] Interviews with practitioners, industry consultants, and field experts. GSMA (2015) *Connected Women: Adaptation Framework for the Mobile Technical Literacy Toolkit*, available at https://bit.ly/314S6MU.
[99] Hassan, B and Unwin, T and Gardezi, A (2017) Understanding the Darker Side of ICTs: Gender, Sexual Harassment, and Mobile Devices in Pakistan, available at https://bit.ly/37NGwqM
[100] For more information, see Section 2.2.4 Technical Literacy, Section 2.2.3 Education, Literacy and Section 2.3.1 Social, Cultural and Economic Divide.

The GSMA created an agent training guide[101] and adaptation framework[102] to build women's mobile technical literacy. It progresses from voice calls to SMS messaging, mobile money and to numeracy skills consumers needed to reasonably and safely conduct financial transactions. While there are strategies for increasing financial and digital literacy, there is scant instruction on methods of increasing women's cybersecurity awareness and hygiene beyond the most basic facts concerning user PINs. Reference was made to capacity building campaigns which occasionally air on radio channels.[103] A training manual for women agents by Bangladesh Bank does provide some emphasis on mobile and DFS security to deal with fraud which address the limitations of customers with lower financial and digital literacy levels.[104]

2.3 Social, Cultural, Economic and Gender Specific Divides

Strong social and cultural influences can define gender norms – expected roles, responses and opportunities – and can act to increase gender inequality and impact on the manner in which women approach and use ICT and DFS. This section elaborates on and examines these issues.

2.3.1 Social, Cultural and Economic Divide

Social and cultural norms define gender roles and expectations. Male family members are often expected to be the breadwinners, possess more freedom and empowerment than females, such as access to and control over financial and technological products and services as illustrated earlier. They may also have the liberties of unrestricted mobility, enjoying greater access to employment opportunities and exposure to the marketplace to experience and interact directly with technology and DFS. Men also spend more time in public spaces where they can access peer knowledge networks – information discussion and information sharing between friends and colleagues.[105] This can include conversations with others at work, cafes or through the use of mobile communications, all of which form the basis of better fraud and cyber awareness, appreciation for cyber hygiene and comfort with technology. (For more information about peer networks, see **Exhibit 9**.)

Women's roles have often been perceived to be as homemakers, expected to spend more time occupying private spaces as managers of the household and primary caregivers of children. Women who are primarily home-based may perceive a limited need for mobile phone use and ownership.[106] As mentioned earlier, women in Kenya have been traditionally steered away from STEM-based opportunities and more towards social sciences and "women's jobs" such as general marketplace opportunities and agriculture.[107]

---

[101] GSMA (2015) *Connected Women: Mobile Skills Toolkit*, available at https://bit.ly/3fHY1vB.
[102] GSMA (2015) *Connected Women: Adaptation Framework for the Mobile Technical Literacy Toolkit*, available at https://bit.ly/314S6MU.
[103] GSMA (2015) *Connected Women: Adaptation Framework for the Mobile Technical Literacy Toolkit*.
[104] Bangladesh Bank (2018) *Women Mobile Financial Services Agent Recruitment Manual 2018.*
[105] Interviews with practitioners, industry consultants, and field experts.
[106] Supplement GSMA report on Women's need to own phones. Wyche, S and Olson, J (2018) *Kenyan Women's Rural Realities, Mobile Internet Access and "Africa Rising"*.
[107] Interviews with practitioners, industry consultants, and field experts.

The importance and impact of family and peer networks as a source of information in developing countries cannot be understated. Especially with regard to women, they can form the basis for decision making in many respects even at the earliest stages, such as what mobile network operator (MNO) to choose and DFS agent to use.[108] The value, breadth and quality of information in the network is representative of its participants. This can be influenced by gender, especially in areas of greater segregation such as in parts of SA.

A substantial part of continued technology and DFS education arises through peer groups and knowledge communications networks resulting from relationships with surrounding people.[109] This includes the freedom to move in public spaces and meet others to engage in rewarding, information-rich experiences such as at work, the marketplace and informal spaces (cafes, shops and social places.) In these environments, as well as online forums and chat apps, substantive and sophisticated technical discussions occur where dynamic information is shared on technology and DFS such as timely warnings about cyber risks, frauds and social engineering scams; how to troubleshoot problems and identify and confirm scams[110]; and navigate and resolve support and grievance mechanisms. This increases overall fraud and cyber awareness, knowledge and confidence. The effectiveness of women's peer referral networks using SMS (relating to purchasing influence) was exemplified in a joint effort in Pakistan to reach and encourage more women to access and use a digital wallet.[111]

Women, especially in the poor and working-class demographic, may have limited experiences engaging with a bank, a financial institution, a digital financial services provider (DFSP), microloan company, and in conduct transactions in the marketplace. The result is that their "peer knowledge networks" with other women can be less useful from an ICT/DFS context and are generally more domestic in nature. Asa consequence, poor women often have technical networks that are inferior to men in terms of reach and level of the sophistication in that these networks tend to lack comparable breadth of discussion and related experience on topics related to cybersecurity practices, awareness and timely warning of frauds.[112]

Exhibit 9: Peer Knowledge Networks
Peer networks are critical information communications between customers, often between those within familiar peer groups and can be influenced by gender in certain regions.

[108] Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC. See also Section 3.5 Agents: Gender Representation and Fraud.
[109] Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC; Interviews with practitioners, industry consultants, and field experts.
[110] "Peer verification" is a common practice of inquiring of colleagues for opinions regarding suspect communications. Williams, JE and Hinds, J and Joinson, A (2008) *Exploring susceptibility of phishing in the workplace*, available at https://bit.ly/3fMOweE.
[111] Sending gender-centric text messages to women encouraging people to refer women to use the JazzCash digital wallet platform increased referrals up to 34% using scalable SMS communications. Ideas42 (2020*) Bringing Digital Finance Tools to More Women*, available at https://bit.ly/3fPORNH.
[112] Interviews with practitioners, industry consultants, and field experts. See also Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh, IFC.*

A World Bank study found that, in ten surveyed countries in SSA and SA, over 70% of women worked in informal employment.[113] In Kenya, where mobile phone ownership among women is among the highest in Africa (83%), women still experience subordinate gender roles, especially in rural areas.[114] The IFC Bangladesh Study found that 81% of rural women were economically dependent on other household members and only 4% were the primary income earners.[115] Women were more likely to own and use mobile phones when they participated in the workforce, although they had limited time for capacity building in needing to manage twin roles of the home and work spaces. They generally had less time and access to public spaces and peer networks which are information rich on topics such as ICT and DFS, and where a substantial amount of information exchange takes place.

In environments where there is a stronger presence of patriarchal, religious and/or conservative social and cultural influences, women may live and exist in space separate from men and create palpable social, cultural and physical and emotional barriers.[116] In countries such as Pakistan and Bangladesh, especially in rural areas, travel distances to key places may be limited and/or restricted[117] such as work opportunities, which may even require familial assent.[118]

As a result of divides, women can be generally less exposed to ICT and DFS and tend to possess less confidence in their abilities and may fear the repercussions of mistakes they make in predominantly male dominated environments.[119] Women must also be cautious about money and financial information which may be visible on shared mobile phones, such as vouchers and cash balances, which other family members

[113] The informal economy includes non-agricultural employment in jobs in "unregistered or small-scale private enterprises that produce goods or service for sale, self-employed street vendors, taxi drivers and home base workers." Ortiz-Ospina, E and Tzvetkova, S and Roser, M (2018) *Women's employment*, available at https://ourworldindata.org/female-labor-supply

[114] Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC. Interviews with practitioners, industry consultants, and field experts.

[115] Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC.

[116] Bangladesh Bank (2018) *Women Mobile Financial Services Agent Recruitment Manual 2018.* Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh*, IFC.; Interviews with practitioners, industry consultants, and field experts. See also Wyche, S and Olson, J (2018) *Kenyan Women's Rural Realities, Mobile Internet Access, and "Africa Rising"*; Sambasivan, N and Batool, A and Ahmed, N et. al. (2019) *"They Don't Leave Us Alone Anywhere We Go": Gender and Digital Abuse in South Asia*.

[117] Social norms may prevent women from travel distances, such as in certain villages in India where such is greatly discouraged by community members, leaving women to rely on others or for their husbands to return to be able to access DFS such as monetary withdrawals. Harsh Pandey, S and Wright, GAN (2015) *Connecting the Dots: Putting Risk, Customer Protection, and Financial Capability in Perspective*; Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC. Regarding Africa and South Asia: "In many countries, only men travel to the market town." Wright, G and Narain, N and Kapoor, R (2020) *Trust Busters! A dozen reasons why your potential customers do not trust your agents (particularly in rural areas)*, available at https://bit.ly/2zVWyTc.

[118] In Bangladesh, women may experience a requirement of a family acceptance and acceptance of her role as a working person as well as limitations on distance travel. There can also be discrimination against women, who present the potential for work interruption due to pregnancy. Bangladesh Bank (2018) *Women Mobile Financial Services Agent Recruitment Manual 2018.*

[119] Bangladesh Bank (2018) *Women Mobile Financial Services Agent Recruitment Manual 2018* Interviews with practitioners, industry consultants, and field experts.

may discover and claim for themselves.[120] As a result, unbanked and undeserved women may have a tendency to be more cautious and risk averse than men.

2.3.2 Gender Imbalances, Women's Confidence and Sexual Harassment

As mentioned earlier, gender inequality is generally higher than global averages in developing countries[121] and can be notably more pronounced in areas of patriarchal, religious and/or parochial influences, such as in Pakistan, Bangladesh and India. [122] The prevalence of sexual harassment and of gender imbalances in the workforce is also notable in these regions, although not confined to them. Encountering a predominantly male workforce when interacting with agents and grievance resolution mechanisms (GRMs) can act to make women apprehensive of using ICT and DFS as well as negatively impacting their attitudes and behavior towards such products and services should they choose to do so.[123]

Women who lose money through DFS – victims of cybersecurity failures, capacity limitations or DFS fraud – can face notable derision. They may be blamed, shamed and ridiculed from family members, friends and even authorities (such as DFS agents, DFSP customer support representatives and police) even when it may not be their fault.[124] This can diminish a woman's confidence in DFS, her abilities[125] and her capacity for dealing with the consequences of failure as feelings of anticipated regret arise in advance of engaging in transactions.[126] These reactions are reasons some posit that women are more likely to be more

[120] Interviews with practitioners, industry consultants, and field experts.
[121] For example, see the reference to the global parity index in Section 2.2.3 Education, Literacy and Numeracy.
[122] Interviews with practitioners, industry consultants, and field experts. See also Sambasivan, N and Batool, A and Ahmed, N et. al. (2019) *"They Don't Leave Us Alone Anywhere We Go": Gender and Digital Abuse in South Asia*; Hassan, B and Unwin, T and Gardezi, A (2017) *Understanding the Darker Side of ICTs: Gender, Sexual Harassment, and Mobile Devices in Pakistan*.
[123] For more information, see Section 3.5 Agents: Gender Representation and Fraud and Section 3.6 Grievance, Resolution Mechanisms.
[124] Women at the BOP often experience lowered levels of confidence and security, high levels of vulnerability. As they are not a primary target consumer by the marketplace, there is little confidence that social institutions and market systems would protect you after being victimized versus being questioned and blamed. Questions from agents, support representatives and even from other family members question: "Why did you give out that information? You, the woman, must have made some type of mistake and are at fault." Interviews with practitioners, industry consultants, and field experts. See also Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC. Microsave (2014) *Survival of the Fittest: The Evolution of Frauds in Uganda's Mobile Money Market (Part-I),* available at https://tinyurl.com/y9u8pq7n. In general, high levels of cybercrime go unreported especially in Africa and South Asia. Surveys by Serianu in 2018 in several African countries yielded the following percentages of people not reporting cybercrimes to the police: Lesotho 88%, Uganda, 72%, Kenya 50%, Botswana 35.4%. See Serianu (2019) *Annual Reports*, available at https://www.serianu.com/annual-reports.html; Victim blaming and shaming is not limited to these regions and has also been reported as an issue of concern in the United Kingdom. National Fraud Authority (2006) *Fraud Typologies and Victims of Fraud*, available at https://bit.ly/2AWK1iO.
[125] The concept of "self-efficacy" is described in Section 3.4.2 Personality and Character Traits.
[126] More information on the concept of anticipated regret can be found in Section 2.3.2 Gender Imbalances, Women's Confidence and Sexual Harassment. Strong social and cultural influences can define gender norms – expected roles, responses and opportunities – and can act to increase gender inequality and impact on the manner in which women approach and use ICT and DFS. This section elaborates on and examines these issues. and Section Social Engineering Methods and Techniques. See also Sommestad, T and Karlzen, H and Hallberg, J (2015) *The sufficiency of the theory of planned behavior for explaining information security policy compliance*, available at https://bit.ly/3djJ0OR; Verkijika, SF (2019) *"If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender*, available at https://bit.ly/3ezTpHT.

risk averse than men regarding situations where security could be comprised and risk of monetary loss are in issue.[127]

Cyber and Sexual Harassment. Harassment of women may present a notable deterrent to their use of and familiarity with ICT and DFS, reducing financial, technical and cybersecurity knowledge and experience. Women in Bangladesh have shared concerns about personal and contact information shared during DFS onboarding[128] and in agent assistance.[129] Once onboarded, many also reported experiencing some form of sexual harassment when using DFS[130] and receiving such phone calls from unknown men.[131]

Studies in Pakistan have recognized that mobile phones are an ideal communication medium for cyber-harassment. Sending text messages or other communications is simple to accomplish: rich media such as photos are easily attached; the victim will usually have the phone in their possession or nearby and there is a higher likelihood of being seen than using other methods;[132] it is capable of attacking from a distance; identity protection of the attacker can be relatively easy to accomplish (such as with call spoofing and where KYC processes are poor.[133] One study of mobile sexual harassment in India, Pakistan, Bangladesh and Cambodia indicated that being a woman translates to 43% higher odds of being harassed than men.[134] A separate study from Pakistan was consistent in reporting that 48% of female versus 18% of male respondents were sexually harassed via their mobile phone, predominantly through SMS, phone calls and social media when connected.[135] Collectively, it is clear that harassment using mobile phones represents a hassle which impacts more women than men and a potential reason for women to avoid or limiting the use of ICT and DFS.

Resolution Mechanisms. Fear of needing to use GRMs can also impact the choice and attitudes of women to use DFS and in reporting – or not reporting – occurrences of fraud in DFS. Employees and officials in the police force and resolution processes of several SA countries are predominantly male.[136] Reporting

[127] Observations have been made in certain populations and results can vary, such as women falling with possibly greater propensity for shopping scams. Interviews with practitioners, industry consultants, and field experts.
[128] For more information, see Section 2.2.1 DFS Onboarding and Section 3.5 Agents: Gender Representation and Fraud.
[129] For more information, see Section 3.5 Agents: Gender Representation and Fraud.
[130] See also women's apprehension of onboarding with predominantly male agents in Section 2.2.1.
[131] Bangladesh Bank (2018) *Women Mobile Financial Services Agent Recruitment Manual 2018.*
[132] SMS text messages have a high open/read rate and viewed quickly. For more information see footnote 209.
[133] Hassan, B and Unwin, T and Gardezi, A (2017) *Understanding the Darker Side of ICTs: Gender, Sexual Harassment, and Mobile Devices in Pakistan*. Anecdotally it was shared consistently by all interviewees that in several countries, especially in South Asia, KYC procedures are often bypassed provided payments are made, such as acceptance of photocopied identification. Interviews with practitioners, industry consultants, and field experts.
[134] Amarasinghe, T (2018) *Policy Initiatives to Address the Problems Faced by Internet & Social Media Users in Relation to Online Harassment in India, Pakistan, Bangladesh & Cambodia*, available at https://bit.ly/3fLPrvP.
[135] 17.5% of respondents were sexually harassed daily through SMS and 54% thought that women who are victims of sexual harassment through her mobile device were usually or sometimes to blame as opposed to 38% for men. Hassan, B and Unwin, T and Gardezi, A (2017) *Understanding the Darker Side of ICTs: Gender, Sexual Harassment, and Mobile Devices in Pakistan*.
[136] For example, the gender composition of the India police force is 92.72% male and just 7.28% female. Common Cause (2019) *Status of Policing in India Report 2019*, available at https://bit.ly/3hPEjjm. As per Section 3.5.1 Gender Representation of Agents , 99% of DFS agents in Bangladesh were male.

fraud or harassment claims to the police often involves leaving personal information and an experience with authorities which women generally lack trust.

A study of women from India, Bangladesh and Pakistan yielded 72% of respondents reporting that they had experienced online abuse but only 1% reported it to police (with help from NGOs),[137] where they faced the potential for additional humiliation in recitation of the facts, providing evidence and details which may not be kept confidential.[138] Fewer than 20% reported these incidents to authority figures including the police and religious and community leaders.[139] Women also face the possibility that they may be blamed for their own victimization,[140] as is examined in Section 3.6. To summarize, key statistics and metrics which would indicate a problem that women face with fraud and GRMs and requiring remedy may be significantly underreported.

3 Cybersecurity and Fraud in DFS: View with a Gender Lens

The issue of how gender may play a role in customer cybersecurity practices and susceptibility to DFS fraud is a complex issue. It can be the product of many factors and influences – social, cultural, biological, and psychological,[141] among others. As opposed to cybersecurity attacks targeting digital devices,[142] social engineering attacks and DFS scams target humans and their behavior patterns, which can be influenced by factors such as gender. Attacking human weakness is the predominant method of cybersecurity attacks in DFS. This Section 3 will examine these topics and explore related gender issues.

---

[137] Sambasivan, N and Batool, A and Ahmed, N et. al. (2019) *"They Don't Leave Us Alone Anywhere We Go": Gender and Digital Abuse in South Asia*.

[138] Interviews with practitioners, industry consultants, and field experts. In India, women report additional humiliation and suffering in reporting sexual harassment crimes at both police stations and hospitals. Human Rights Watch (2017*) "Everybody Blames Me" Barriers to Justice and Support Services for Sexual Assault Survivors in India*. The gender composition of the India police force is 92.72% male and just 7.28% female. Common Cause (2019) *Status of Policing in India Report 2019*.

[139] Hassan, B and Unwin, T and Gardezi, A (2017) *Understanding the Darker Side of ICTs: Gender, Sexual Harassment, and Mobile Devices in Pakistan*. In the course of research, we noticed that the Kenya Internal Affairs Unit (who investigate complaints against police from members of the police force and/or public) recorded a gender breakdown of complainants as 77% by men with only 18% by women and 5% from institutions. Further research as to a correlation was beyond the scope of this study. National Police Service, Internal Affairs Unit (2019) *Performance Report 2019*, available at https://www.iau.go.ke/wp-content/uploads/2020/06/IAU-PERFOMANCE-REPORT-2019.pdf

[140] "It was mentioned that 10,000 complaints have been raised at the police and the number is increasing and that an increasing number of cases were being brought to court. However, it was also stated that victims, mainly women, are hesitant to report cases as they fear this would continue their social defamation." NRD Cyber Security and Global Cyber Security Capacity Centre (2018) *Cybersecurity Capacity Review, Bangladesh August 2018*, available at https://bit.ly/37NDMK6; Studies of Pakistan, Bangladesh and India indicate that women are significantly concerned as being targets for sexual harassment and abuse and possess fear of blame and shame as victims of these abuses. Sambasivan, N and Batool, A and Ahmed, N et. al. (2019) *"They Don't Leave Us Alone Anywhere We Go": Gender and Digital Abuse in South Asia*; Hassan, B and Unwin, T and Gardezi, A (2017) *Understanding the Darker Side of ICTs: Gender, Sexual Harassment, and Mobile Devices in Pakistan*

[141] Cislaghi, B and Heise, L (2020) G*ender norms and social norms: differences, similarities and why they matter in prevention science*, available at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7028109/; Todd, B and Fischer, R and Di Costa, S et. al. (2017) *Sex differences in children's toy preferences: A systematic review, meta-regression, and meta-analysis*, available at https://onlinelibrary.wiley.com/doi/epdf/10.1002/icd.2064; See also https://bit.ly/3ae6DKk and https://bit.ly/3jKa3aY.

[142] Baur-Yazbeck, S (2018) *4 Cyber Attacks that Threaten Financial Inclusion*; and Buku, M and Mazer, R (2017) *Fraud in Mobile Financial Services: Protecting Consumers, Providers, and the System*.

While a comprehensive study of the profile of cybercriminals was not conducted, industry experts and sources we consulted were consistent in the observation that there is a higher likelihood of cyber attackers being comprised of males.[143] Selection of victims of cyber attackers were dependent on the type of crime perpetrated, with financial crimes potentially being non-gender specific and more dependent on data harvesting sources, such as from insecure building registries in countries such as Kenya[144] and the use of technology to send electronic messages in bulk (discussed in Section 3.3.2.)

3.1 Cybersecurity: Regional Perspective

While the number of cybersecurity attacks worldwide have grown substantially, the 2017 ITU Cybersecurity Index reported a lagging national response, with only 38% of member countries having a cybersecurity strategy with the lowest commitment level in SSA.[145] The African region contains the largest volume of mobile money transfers[146] and customers but industry and respective technologies ostensibly lag well behind the current state of cybercrime advancement.[147] An African cybersecurity firm estimated that cybercrime costs the region USD 3.5 billion annually and a survey suggested that a substantial majority of African businesses operate well below acceptable cybersecurity practices.[148] A 2018 survey of six African countries by the Global Cybersecurity Capacity Centre (GCSCC) noted that all lacked a national cybersecurity awareness program and described efforts as being in an embryonic stage with "extremely low ICT literacy levels which hinder any design of cybersecurity campaigns and that executive

[143] In addition to anecdotal evidence, see Uganda Police (2019) *Annual Crime Report 2018*, available at https://www.upf.go.ug/wp-content/uploads/2019/05/annual-crime-report-2018..pdf; Uganda Police (2020) *Annual Crime Report 2019*, available at https://www.upf.go.ug/wp-content/uploads/2020/04/Annual-Crime-Report-2019-Public.pdf?x45801; Donner, CM (2016) *The Gender Gap and Cybercrime: An Examination of College Students' Online Offending, Victims & Offenders*, 11:4, 556-577, available at https://bit.ly/3nwSmg6; Hadzhidimova, LI and Payne, BK. (2019) *The profile of the international cyber offender in the U.S.*, International Journal of Cybersecurity Intelligence & Cybercrime: 2(1), 40-55, available at https://vc.bridgew.edu/ijcic/vol2/iss1/4; There is a significant belief that cybercrime is predominantly conducted by males, which is often interpolated from a variety of factors such as gender distribution of cybercrime prosecutions, attendees at hacker conferences, participants in stem programs, etc." Hutchings, A and Chua, YT (2019) *Gendering Cybercrime*, available at https://bit.ly/37RE1DO; Schell, BH and Melnychuk, J (2010). *Female and Male Hacker Conference Attendees: Their Autism-Spectrum Quotient (AQ) Scores and Self-Reported Adulthood Experiences*, available at https://www.igi-global.com/gateway/chapter/60997; Taylor, P (1999) *Hackers: Crime and the Digital Sublime*, available at https://bit.ly/3fOHJBd; Taylor, P (2005) *From hackers to hacktivists: speed bumps on the global superhighway?*, available at https://bit.ly/2YlecZI.

[144] Several of our interviewees noted that a popular data source for smishing and vishing attacks were from unsecured building registries, where security mandates required that entrants provide their name, telephone number and signature. See also reference to black market purchases of data in footnote 193.

[145] UN (2017) *Half of all countries aware but lacking national plan on cybersecurity, UN agency reports*, available at https://bit.ly/2YmOwfj.

[146] Symantec and the African Union Commission (2016) *Cyber Crime & Cyber Security: Trends in Africa. Global Forum for Cybersecurity Expertise Initiative*, available at https://bit.ly/31egbBg.

[147] SWIFT (2017) Force Shaping the Cyber Threat Landscape for Financial Institutions, Working Paper 2016-004, available at https://bit.ly/2B5dUxs.

[148] Serianu (2017) *Demystifying Africa's Cyber Security Poverty Line*, available at https://bit.ly/2Yn9RFK.

members in organizations myopically underestimate the problem."[149] It would appear that greater priority should be placed in the cybersecurity sector for developing countries, especially as the new era of smartphones advances and will create further challenges for consumers who may possess notably lower levels of technical literacy and cybersecurity awareness.[150]

3.2 Cybersecurity Issues, Awareness and Practices

The concept of cybersecurity awareness is bipartite: being aware of the cybersecurity risks and also understanding how to address them.[151] Women in many developing countries still primarily access DFS through basic or feature phones, communicating and interacting through voice, text and USSD-based DFS transactions.[152] The sum of cybersecurity and fraud issues is narrower in comparison to smartphones (which involve proper management of a myriad of app and system settings) but still of significant concern. As illustrated in Section 2, women in developing countries – especially those in the BOP in rural areas – exhibit substantially lower mobile phone ownership, literacy, educational, financial and technical literacy levels as compared to men. Accordingly, their levels of cybersecurity and fraud awareness are likely to be comparatively low, with observations and examples of such challenges summarized below:

- Women in the BOP in rural areas may generally lack awareness and knowledge about basic DFS product and service information, pricing, and resolution mechanisms;[153]
- Cyber awareness and technical capacity of women is likely low at the time of onboarding; customer education may be limited at the agent level as focus is often primarily on sales with basic attention to security training; family members may supplement cyber awareness to a moderate degree; [154]
- While MNOs, DFSPs and governmental authorities related to ICT may attempt to push information to the masses with regard to cyber awareness and hygiene, it is often limited in effectiveness and very low on the grassroots level.[155]
- Cyber awareness and technical capacity of women may remain lower than men after onboarding as women's peer knowledge networks – a critical component of post-onboarding support – are typically not as robust, informative and substantive as men's networks;[156]

---

[149] Bada, M and Von Solms, B and Agrafiotis, I (2018) *Reviewing National Cybersecurity Awareness in Africa: An Empirical Study*, available at https://bit.ly/3dhZZB3; Using Bangladesh as an example, it did not have a sufficient legislative framework for ICT security at the time of a 2018 study. NRD Cyber Security and Global Cyber Security Capacity Centre (2018) *Cybersecurity Capacity Review, Bangladesh August 2018*.

[150] SWIFT (2017) Force Shaping the Cyber Threat Landscape for Financial Institutions, Working Paper 2016-004.

[151] NRD Cyber Security and Global Cyber Security Capacity Centre (2018) *Cybersecurity Capacity Review, Bangladesh August 2018*.

[152] See Section 2.1 The Digital Gender Divide: Mobile Access, Handsets and Usage.

[153] See Section 2.2.2 reporting that, in the IFC Bangladesh Study on women, 20% or less were aware of DFS fees and costs and customer rights. Many also were unaware of GRM, examined in Section 3.6.

[154] As in Section 2.2.4 Technical Literacy, the GSMA agent training manual indicates a minimum of attention on cybersecurity awareness and best practices for customers. Industry experts and MNO employees interviewed were consistent in observing customer onboarding training consisting primarily of revenue generating activities such as teaching users product and services features. Basic PIN education was shared. As women in the BOP are sensitive to fraud vulnerability, focus at onboarding was perceived as a significant potential deterrent. Interviews with practitioners, industry consultants, and field experts.

[155] This was an opinion shared unanimously among all industry experts and consultants we interviewed.

[156] For more information, see **Exhibit 9**.

- A sizable segment of women consists of DFS proxy users, dormant account holders or the unbanked who often use agent-assisted OTC transactions and can substantially increase the risk and potential for cybersecurity breaches, fraud and identity theft;[157] this risk may be exacerbated by challenges of limited literacy and awareness of proper DFS and security practices;[158]
- Shared phones, more popular among women, create greater cybersecurity risk as personal contacts, text messages, sensitive information, transaction notices, and rich media are potentially exposed and likely accessible to and viewable by other users;[159]
- Women's interaction with technology can more often necessitate reliance on assistance from others as they may not possess the requisite skills (or confidence in their skills) to navigate successfully. Women in different jurisdictions have shown an inclination to put blind trust in agents (and sometimes others) such as PIN sharing during assistance, which can facilitate fraud.[160] (See **Exhibit 10** for an illustration);
- Adult women's lower literacy and numeracy levels impact on their basic understanding of the financial and technical parts of DFS and may be further compounded when English is used for DFS and is not provided in the customer's native language;[161]
- Customer onboarding and GRM requires women to provide private information, phone numbers, photographs (for KYC, sometimes GRM); A disproportionate and predominantly male representation of agents or employees may increase risks of information disclosure and sexual harassment, especially in jurisdictions lacking adequate cyber law and regulation.[162]

[157] For more information about OTC transactions, see Section 3.5.3 Agent Fraud and Misappropriation.
[158] Proxy users are those whose accounts are used by another person, usually a family member such as a woman's husband. For more information, see Microsave (2019) *The real story of women's financial inclusion in India*.
[159] For more information see Section 2.1.2 Phone Ownership and Sharing.
[160] Harsh Pandey, S and Wright, GAN (2015) *Connecting the Dots: Putting Risk, Customer Protection, and Financial Capability in Perspective*; Bangladesh Bank (2018) *Women Mobile Financial Services Agent Recruitment Manual 2018.* Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh*, IFC; For additional information, see also Section 3.5.3 While not encouraged in Sri Lanka and is more recently being discouraged in India. Riley, TA and Kylathunga, A (2018) *Bringing E-money to the Poor: Successes and Failures,* World Bank, available at https://tinyurl.com/ycrfdpem. For more information on PIN sharing with strangers by women in India, see **Exhibit 8**.
[161] Women in Bangladesh struggle to understand English USSD menus, which can result in erroneous DFS transfers. Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC.
[162] Human Rights Watch (2017*) "Everybody Blames Me" Barriers to Justice and Support Services for Sexual Assault Survivors in India*. The gender composition of the India police force is 92.72% male and just 7.28% female. Common Cause (2019) *Status of Policing in India Report 2019*, available at https://bit.ly/3hPEjjm Bangladesh and India are two of several jurisdictions which are lacking in legal and regulatory coverage for cybercrime and cybersecurity. NRD Cyber Security and Global Cyber Security Capacity Centre (2018) *Cybersecurity Capacity Review, Bangladesh August 2018*; Klugman, J (2017) Gender based violence and the law, available at https://bit.ly/2zY8L9M.

- Automatic and Unread SMS Transmissions[163] – such as ignoring text messages – is an increasingly common practice among women with low literacy levels which can make important and timely security warnings and alerts ineffective;[164]
- Generally speaking (and gender neutral), the compact nature and limited size displays of mobile phones can create inherently strong cybersecurity challenges to users.[165]

[163] There has been an increase in digital products being offered in developing countries (such as automated opt-in governmental insurance programs in India) that has led to the usage of a larger number of SMS text messages which may not be recognized or understood by consumers.

[164] This happened often in India. Good cybersecurity awareness and general practices includes appreciating (i) where transactions are happening, and (ii) whether the transactions are correct. Interviews with practitioners, industry consultants, and field experts.

[165] Bada, M and Von Solms, B and Agrafiotis, I (2018) *Reviewing National Cybersecurity Awareness in Africa: An Empirical Study*; As referenced in Section 3.3.2.2 Smishing: SMS-Based Phishing, the high read rate of SMS messages and the urgency factor makes mobile phones ideal for committing social engineering frauds. The limited size of mobile screen is optimal for social engineering methods, such as the abbreviation of text and hyperlinks that appear in Internet browsers among other similar issues. Lookout (2018) *Mobile phishing 2018: Myths and facts facing every modern enterprise today*, available at https://bit.ly/2Z2E38e.

A study by MicroSave of women working in an R&D factory in a peri-urban area in India exemplified women's potential vulnerability relating to cybersecurity and DFS – a visceral lack of self-confidence and fear of making mistakes which resulted in reliance on unknown persons for assistance.[166] The women were well trained, educated, and consisted of married and unmarried. At least 57% said that they required assistance when they wanted to transact at an automated teller machine (ATM). The most significant challenge these women faced was a deep-rooted lack of confidence to use ATMs. 48% responded to the survey admitting that they share PIN codes with helpers at the ATM kiosk locations – the known "clubhouse for fraudsters" – and many of these women became theft victims. This type of conduct pattern was observed in women regionally outside of India as well, who also share PIN codes because they feel a strong need for help and, for reasons not fully explained, believe that they can trust the helper.[167]

Exhibit 10: Women's Cybersecurity Awareness and Confidence Using DFS

3.3 Social Engineering

Social engineering is an attack on humans – rather than machines – who control access and authorization to electronic data, information and computer networks. It is the art of manipulating people into performing a desired action under false pretenses, often for the purpose of reaping financial reward. Social engineering presents a cyberattack that frequently affects DFS. It relates to human behavior which can be influenced by gender factors, which are examined in this section.[168]

3.3.1 Social Engineering Methods and Techniques

The increase of social engineering attacks, especially in developing countries,[169] may be rooted in its relatively low barriers to entry, efficiency and scalability.[170] It relies less on the technological skills (and gender)[171] of the attacker and more on exploiting basic human psychology[172] – anticipating how a population tends to react to specific situations. Attacks may be optimized, tailored and refined over time for a target population, such as a poorer, less educated group of persons in a developing country who may predominantly use basic and feature phones. Regional consultants, central banks and MNOs we consulted repeatedly emphasized social engineering as a predominant problem confronting DFS users and providers

[166] See Pandey, S and Wright, GAN (2015) *Connecting the Dots: Putting Risk, Customer Protection, and Financial Capability in Perspective*, available at https://bit.ly/3djaVi5.
[167] Interviews with practitioners, industry consultants, and field experts. See also Hudson Matthews, Brett (2010) *Orality and Microsavings*.
[168] Baur-Yazbeck, S and Frickenstien, J and Medine, D (2019) *Cyber Security in Financial Sector Developing: Challenges and potential solutions for financial inclusion*, available at https://bit.ly/3exl0sZ
[169] Agoi, G (2020) *Cybersecurity Threat landscape in Kenya 2019 and the remedy*, MTN, available at https://bit.ly/2YmP057. SWIFT (2017) Force Shaping the Cyber Threat Landscape for Financial Institutions, Working Paper 2016-04.
[170] The Federal Bureau of Investigation (**FBI**) Internet Crime Complaint Center (IC3) reported that, in the US, social engineering consisted of 25% of all cybercrimes reported and that India, South Africa and Malaysia ranked 3, 13 and 18, respectively, in the top 20 international cybercrime victim countries. IC3 (2020) *Internet Crime Report*, available at https://pdf.ic3.gov/2019_IC3Report.pdf
[171] There appears to be a persistent belief that cybercrimes are still predominantly perpetrated by males. See Footnote 143
[172] Lohani, S (2018) *Social Engineering: Hacking into Humans*, available at https://bit.ly/2V4VDHq.

due to low levels of digital literacy, cyber awareness and cyber hygiene present locally and the simplicity and effectiveness of the attacks.

Social engineering attack vectors include phishing (generally referring to Internet e-mail), "smishing" (SMS-based text message phishing), "vishing" (voice-based phishing) and pretexting (also known as "impersonation"), which are examined in greater detail in Section 3.3.2.

Many phishing attacks, especially smishing and which is common in DFS, often consists of two stages: (i) a bad actor who masquerades as a legitimate party who communicates a message to the victim with a call to action (ii) which is intended to elicit an expeditious or urgent response by the victim.[173] Time-limited or urgent communications are designed to divert the user's attention away from noticing specific message details that would indicate its deceptive nature and towards a compelling need for urgency in responding[174] – such as to avoid missing out on the collection of a valuable reward.[175] The concept of urgency is one of several "influence techniques"[176] commonly used to effectuate social engineering scams in the context of DFS.[177] A select list includes:

- **Authority.** The tendency of people to follow messages sent by a recognizable authority;
- **Reciprocity.** The tendency for people to feel obligated or eager to return favors;
- **Social Proof.** The tendency of people to comply with or feel that an opportunity is safe when it is implied others have participated safely;
- **Sympathy.** The natural inclination people may have to assist those in need.
- **Scarcity/Reward.** The tendency of people to comply or respond to communication when there is a belief that a rare opportunity may exist;
- **Urgency.** The tendency of people to act when presented with a limited time to potentially obtain a benefit or to avoid a loss.

These influence techniques have been used to create several popular social engineering frauds which have become prevalent in developing countries and affect DFS customers. Based on our interviews and review of available studies, we have divided common DFS related frauds or scams into two primary categories,

[173] Broadhurst, R and Skinner, K et. al. (2020) *Phishing and cybercrime risks in a university student community*, available at https://bit.ly/2Bqo1N6; Salahdine, F and Kabouch, N (2019) *Social Engineering Attacks: A Survey*, available at https://bit.ly/3enQwK0.

[174] Communications are "designed to enact peripheral rather than central information processing." Norris, G and Brookes, A and Dowell (2019) *The Psychology of Internet Fraud Victimisation: a Systematic Review*, available at https://tinyurl.com/ybt8557v.

[175] Vishwanath, A and Herath, T and Chen, R et. al. (2011) *Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing mode*l, available at https://tinyurl.com/yclgv5qh; Broadhurst, R and Skinner, K et. al. (2020) *Phishing and cybercrime risks in a university student community*; Salahdine, F and Kaabouch, N (2019) *Social Engineering Attacks: A Survey*, available at https://www.mdpi.com/1999-5903/11/4/89; Williams, E and Hinds, J and Joinson, A (2008) *Exploring susceptibility of phishing in the workplace*, available at https://tinyurl.com/ycq4xr3o.

[176] Williams, JE and Hinds, J and Joinson, A (2008) *Exploring susceptibility of phishing in the workplace*; Bleiman, R and Rege, A (2018) *An Examination in Social Engineering: The Susceptibility of Disclosing Private Security Information in College Students*.

[177] A collection of scientific and academic studies appears in Section 3.4.2 Personality and Character Traits.

those being where victims are deceived into: (1) theft of funds – remitting funds directly to the fraudster; and (2) theft of information – divulging sensitive information, data or identity.[178] These frauds are examined below.

3.3.1.1 Theft of Funds

Frauds in this section use a similar strategy. Repeated attacks are made to induce relatively small payments from victims, profiting through transaction volume. The amounts requested are sufficiently modest to fall under levels which would raise internal alarms and likely to be dismissed by victims after discovery due to the considerable investment and effort necessary to pursue a potentially unsuccessful remedy.[179] The most common forms of these theft of funds include the following:

- **Advance Fee Scams.** A victim is lured by an ostensible opportunity to receive a considerable gain by remitting a much smaller amount – an advance fee – to preserve an opportunity or to effectuate the transfer of a non-existent windfall.[180] Common schemes include the victim receiving notice of winning a lottery, prize, loyalty benefit from an MNO or DFSP or a package sent from a relative or vendor. In each of these examples some type of small advance fee is required to be paid by the victim, such as a modest deposit or processing and/or shipping fee. (For a current example, see the COVID-19 smishing scam in **Exhibit 12**, appear in Section 3.3.2.2.)
- **Purported Wrong Transfer.** A fraudster transmits a fake money transfer notification to the victim, usually via SMS. It is followed by a subsequent message explaining that the transfer was sent in error to the wrong customer number with a request for remittance back of the funds. Impulsively, the victim may remit money to the sender without a prior review and confirmation that a transaction had actually occurred.[181] Results reported in the IFC Bangladesh Study numbers suggest that women might be more susceptible to being victimized by this scam than men.[182]

---

[178] While the relevant studies were examined, they depart in numerous respects from the DFS environment. See Section 3.4 Gender, Cybersecurity and Fraud Studies. Furthermore, "[t]he majority of evidence and subsequent beliefs we have regarding the psychological factors associated with vulnerability to online fraud are at best anecdotal and at worst in danger of creating misleading myths." Norris, G and Brookes, A and Dowell (2019) *The Psychology of Internet Fraud Victimisation: a Systematic Review*.

[179] Gerke, M (2011) *Understanding Cybercrime: A Guide for Developing Countries*, available at https://tinyurl.com/yaqwzmz2. See also grievance resolution mechanisms in Section 3.6. Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC. Mudiri, JL (2012) *Fraud in Mobile Financial Services*, available at https://tinyurl.com/y98e5j9x; Microsave (2014) *Survival of the Fittest: The Evolution of Frauds in Uganda's Mobile Money Market (Part-I);* Phiri, P (2019) *In Zambia, Scams on the Rise as Mobile Money Booms*, available at https://tinyurl.com/y9olhvus. Interviews with practitioners, industry consultants, and field experts.

[180] Gerke, M (2011) *Understanding Cybercrime: A Guide for Developing Countries*; Ayettey, L T (2019) *Momo fraud: How scammers steal your money*, available at https://tinyurl.com/y7ogulcz; Microsave (2014) *Survival of the Fittest: The Evolution of Frauds in Uganda's Mobile Money Market (Part-I),* available at https://tinyurl.com/y9u8pq7n.

[181] Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC. Mudiri, JL (2012) *Fraud in Mobile Financial Services*, available at https://tinyurl.com/y98e5j9x; Microsave (2014) *Survival of the Fittest: The Evolution of Frauds in Uganda's Mobile Money Market (Part-I);* Phiri, P (2019) *In Zambia, Scams on the Rise as Mobile Money Booms*, available at https://tinyurl.com/y9olhvus. Interviews with practitioners, industry consultants, and field experts.

[182] The IFC Bangladesh Study noted that over 50% of women had sent money to a wrong account, potentially from errors relating to lower literacy and technical skills, English language proficiency and low DFS familiarity. Coupled with poor mobile

- **Assistance or Sympathy Scam.** The fraudster communicates an emotional plea for an urgent transfer of funds to assist the sender or the sender's family member in a dire situation, such as for urgently needed medical care. The message can take the form of a purported wrong transfer (e.g. money was sent money to the wrong account, intended for the hospital); or purportedly from a friend in need (impersonation); or from a stranger in need of a good Samaritan, preying on the goodwill and nature of the victim who receives the plea.[183]
- **Extortion Scam.** The fraudster informs the victim that they will be harmed in some fashion unless they remit a payment. In the context of gender, especially pertinent to SA where a woman's reputation is of utmost concern, this often translates into a threat to reveal sensitive private details, e.g. knowledge or photos relating to an embarrassing incident, etc.

Anecdotal evidence and some relevant studies loosely suggest that unbanked and underserved women in Africa and SA may exhibit tendencies to be more compliant with authority and sympathetic towards others.[184] and more risk averse than men.[185] Men were observed to be victimized more often by advance fee and lottery scams.[186] It is important to note that results can vary within different regions, population demographics, cultures, and other factors comprising of this complex subject, some of which are reviewed in the studies contained in Section 3.4.

3.3.1.2 Identity Theft, Data Theft, SIM Swaps

An attacker may use social engineering techniques to induce a person, through deception, into unwittingly disclosing sensitive information (such as a PIN) and/or authorizing an act (such as an account approval.)[187]

phone quality (which can increase accidental keypresses), the authors hypothesize that women may be particularly vulnerable to purported wrong transfer scams. Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC; Wyche, S and Olson, J (2018) *Kenyan Women's Rural Realities, Mobile Internet Access, and "Africa Rising"*.

[183] Van Rensburg, KSJ (2017) *The human element in information security : an analysis of social engineering attacks in the greater Tshwane area of Gauteng, South Africa*, available at https://tinyurl.com/y7umo75y; Ayettey, L T (2019) *Momo fraud: How scammers steal your money*, available at https://tinyurl.com/y7ogulcz.

[184] Bangladesh Bank noted that women generally display higher levels of empathy, making them ideal agents, most capable of establishing a rapport of trust with DFS customers of all genders. Bangladesh Bank (2018) *Women Mobile Financial Services Agent Recruitment Manual 2018.* Interviews with practitioners, industry consultants, and field experts.

[185] It is suggested that women may more readily perceive consequences and conjure anticipatory regret when directly confronted by the repercussions of loss of funds. Interviews with practitioners, industry consultants, and field experts.

[186] National Fraud Authority (2006) *Fraud Typologies and Victims of Fraud*; Interviews with practitioners, industry consultants, and field experts.

[187] See Section 3.3.2.4 Pretexting / Impersonation. *4 Cyber Attacks that Threaten Financial Inclusion*; Farooq, S (2019) *Mitigating common fraud risks: Best practices for the mobile money industry*, GSMA. In addition to social engineering, information can be stolen due to an organization breach, internal fraud or accessed without permission through the unsecured use of the Internet or downloading of malware.

Identity fraud[188] or identity theft occurs when such disclosed information can be used for personal identification[189] purposes to impersonate the victim. This is often a precursor to a subsequent act which uses the data to commit one or more financial frauds. DFS customers are commonly duped into disclosing their PIN and other sensitive information by fraudsters posing as MNO representatives seeking to "confirm" the subscriber's identity to provide them with a special award, upgrade[190] or in response to technical support pretexts – as is illustrated below in **Exhibit 11**.

A woman in India was the victim of a USD14,000 SIM swap fraud via a vishing and "pretexting" attack. A voice call, purportedly from a sincerely concerned customer care representative of her MNO, informed the woman that her 3G service was being phased out in favor of 4G and would cease working imminently. She was convinced to initiate an "upgrade" request for a SIM swap with her carrier to the newly provided 4G service and informed that a short service interruption of several hours should be expected. During that time, the fraudster completed the SIM swap to a SIM in their control and liquidated her linked financial accounts.[191]

Exhibit 11: SIM Swap Fraud Using Vishing and Pretexting

SIM Swaps and Account Takeover. Swapping out defective SIMs for customers is a common MNO practice. SIM swap fraud occurs when an MNO is convinced to switch a customer's service to a SIM card possessed by a fraudster, often by a fraudster using a PIN code or other sensitive information[192] obtained through identity theft[193] to impersonate of the customer. After seizing the customer's mobile account, the fraudster can siphon funds, airtime and value from that account as well as all linked accounts, and

[188] The Home Office Identity Fraud Steering Committee in the UK distinguishes identity theft as being the case where the fraudster permanently takes on the identity of the victim while identity fraud is temporary, e.g. such as for the purpose of executing a SIM swap fraud or emptying the mobile money accounts of the victim using their identification information. NFA Report.

[189] Examples of government issued identification numbers includes an Aadhaar number in India or a social security number in the U.S.

[190] For more information see smishing, vishing and pretexting in Section 3.3.2 Social Engineering Attack Vectors.

[191] *SIM Swap Fraud: Noida Woman Loses RS 9.5 Lakh by Upgrading SIM from 3G to 4G*, available at https://tinyurl.com/yb6py37b; See also Salahdine, F and Kabouch, N (2019) *Social Engineering Attacks: A Survey*. Kareithi, A (2018) *How tech savvy crooks use your mobile phone line to rob you*, available at https://tinyurl.com/y73d7ka4; Sarang (2019) *SIM swap fraud: What you should know*, available at https://bit.ly/3fTigGG.

[192] If the fraudster doesn't obtain the customer's PIN, a unique SIM card number, mobile money PIN or other personally identifiable information which can be used in a combination of other customer data to be sufficient to effectuate a SIM swap with a mobile carrier. Sarkar, D (2018) SIM Swap Fraud: 13 things you must know about this online banking scam, available at https://tinyurl.com/y99jm6m9Mobile services customers regularly replace or "swap" a lost, stolen or damaged SIM cards for replacements. For more information on "impersonation" or pretexting attacks, see Section 3.3.2.4.

[193] Fraudsters may gather sufficient customer information from phishing techniques, scouring online sources and/or purchasing information from the black market. Business Tech (2019) *Beware these types of fraud, says MTN*, available at https://tinyurl.com/y78ef3mr; Nigeria Communications Week (2018) *Experts Finger Insiders in Telcos for Rising SIM Swap Fraud*, available at https://tinyurl.com/ycythr9y; Makin, P (2018) *Cybersecurity for Mobile Financial Services: A Growing Problem*, available at https://tinyurl.com/y7v7xzej.

potentially apply for credit or other services using the identity of the victim.[194] Social engineering techniques can also be used to exploit vulnerabilities in the two-factor authentication (2FA) process to effectively hijack a user's account.[195]

SIM swap fraud is a pervasive global problem, especially in developing countries where DFS customers are poor and have virtually no loss tolerance.[196] Large scale attacks are occurring in developing countries,[197] including South Africa where reported attacks doubled in one year.[198] The largest bank in Mozambique reported over 17 average SIM-swap frauds each month.[199] Sometimes fraudsters can obtain sensitive customer information with a fraudster resulting from collusion with internal MNO employees, which has been a visible problem.[200] Recently, Safaricom launched its "Tuwaanike" service to combat SIM swap fraud which provides additional notification and an ability for subscribers to opt out of any unknown SIM swap requests.[201]

3.3.2 Social Engineering Attack Vectors

Four primary attack vectors for perpetrating social engineering fraud – phishing, smishing, vishing and pretexting – threaten DFS and financial inclusion,[202] and are examined below in this section.

[194] Baur-Yazbeck, S (2018) *4 Cyber Attacks that Threaten Financial Inclusion*.
[195] After the swap is complete, the scammer has full control of the user's phone service, including access to text messages which are typically used for one-time passwords (OTPs) to complete 2FA. Kan, M (2019) *Google: Phishing Attacks That Can Beat Two-Factor Are on the Rise*, available at https://tinyurl.com/ybcpl82h; Assolini, F and Tenreiro, A (2019) *Large-scale SIM swap fraud*, available at https://tinyurl.com/yab7yd8e.
[196] Estimated costs to fraudsters are typically $10-40 with the potential to generate in excess of $2,500 per victim on average. Kaspersky (2019) *SIM swap fraud: A New Wave of Attacks Targeting Financial services and online services in Africa*, available at https://tinyurl.com/ycf3zaas
[197] Assolini, F and Tenreiro, A (2019) *Large-scale SIM swap fraud*.
[198] SABRIC, a not for profit entity formed by South African banks to combat cyber crime in the banking industry reported a 104% increase in SIM-swap fraud for the first 8 months of 2018. SABRIC (2018) *Digital Banking Fraud Statistics*, available at https://tinyurl.com/y92npbm4; Kaspersky Labs (2019) *SIM swap fraud: A New Wave of Attacks Targeting Financial Services and online services in Africa*, available at https://tinyurl.com/ybge7dq9.
[199] Assolini, F and Tenreiro, A (2019) *Large-scale SIM swap fraud*.
[200] Njeru, B (2018) Safaricom employee, two others arrested over SIM swap fraud, available at https://tinyurl.com/y7d2dut2. Insider attacks responsible for SIM swap fraud also occurs in G7 countries. Francheschi-Bicchierai, L (2019) *AT&T Contractors and a Verizon Employee Charged With Helping SIM Swapping Criminal Ring,* available at https://tinyurl.com/yyhjoo7d.
[201] Jackson, E (2020) *Safaricom Tackles Fraud in Latest MPESA Update*, available at https://tinyurl.com/y9vq3m5x; Otiento, D (2020) *Safaricom will now notify you if someone tries to register a line with your ID Number*, available at https://tinyurl.com/yamyjaoa
[202] Baur-Yazbeck, S (2018) *4 Cyber Attacks that Threaten Financial Inclusion*; Farooq, S (2019) *Mitigating common fraud risks: Best practices for the mobile money industry*, GSMA; Baur-Yazbeck, S and Frickenstien, J and Medine, D (2019) *Cyber Security in Financial Sector Developing: Challenges and potential solutions for financial inclusion*.

3.3.2.1 Phishing: Internet-based E-mail

Phishing[203] is generally understood as the process of casting lures using Internet e-mail to deceive recipients into disclosing sensitive information or providing access to a secured environment,[204] often accomplished by inducing the recipient to click on a hyperlink.[205] Mobile phones represent ideal hardware for phishing frauds. They are portable, often carried by and instantly accessible to users, and data is often adapted and abbreviated to fit small screen sizes which can hide important details and confuse users – such as URLs hidden or abbreviated and conceal URL and domain spoofing.[206]

There exists a myriad of phishing definitions, which is frequently used as an umbrella term to describe the attack mechanism in several vectors. Along with pretexting scams (covered in Section 3.3.2.4), SMS and voice phishing are often used to defraud people in developing countries using basic and feature phones.

3.3.2.2 Smishing: SMS-Based Phishing

Smishing[207] (sometimes appearing as "SMiShing") is an SMS-based social engineering attack that is highly popular in developing countries since all mobile phones and accounts are capable of sending and receiving text messages. Like e-mail phishing, smishing can be efficient, scalable, cost-effective, automated and capable of bulk messaging, with campaigns designed to reach the maximum number of victims with a minimum time invested.[208] SMS messaging can be an ideal attack as text messages have, in comparison to other mediums of communication, the highest open/read rate; are often viewed quickly;[209] have a high response rate; and inherently exhibit the urgency factor which can increase success rates.

---

[203] "Phishing" is a neologism combining "fishing" and "phreaking," a telephone hack which enabled fraudsters to use an electronic "blue box" device to avoid paying for telephone calls. Encyclopedia Britannica (2020) *Phreaking*, available at https://www.britannica.com/topic/phreaking; Kay, R (2004) *Sidebar: The Origins of Phishing, Computerworld*, available at https://tinyurl.com/y9lr6cto

[204] There is no consensus on the definition of "phishing", whose origin is examined in footnote 203. Accordingly, a simple NIST inspired definition has been constructed using the context of DFS. NIST (2020) *Phishing*, available at https://tinyurl.com/yaq5a5pf.

[205] Message formats will depend upon the type of social engineering influence technique used and may include a request to a reply, an attachment which contains malware, an embedded hyperlink which may redirect the user to download malware or a hyperlink to a replica website within which a unsuspecting user may expose their sensitive information. Software Engineering Institute (2014) *Unintentional Insider Threats: Social Engineering*, available at https://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_77459.pdf

[206] Also called "address bar spoofing", a malicious URL can be made to resemble a legitimate and recognizable URL or domain to perpetuate online fraud. Trend Micro (2020) Address bar spoofing, available at https://bit.ly/31fyhTa; Lookout (2018) *Mobile phishing 2018: Myths and facts facing every modern enterprise today*.

[207] The term was first used by David Rayhawk in the McAfee Avert Labs blog in 2006. See Blau, J (2006) *McAfee Warns of SMiShing Attacks, PC World*, available at https://www.pcworld.com/article/126932/article.html.

[208] Maulany, R and Yuyun, S (2017) *Comparative Analysis of Social Engineering Attack Based on SMS and Phone*; Mishra, S and Soni, D (2019) *Smishing Detector: A security model to detect smishing through SMS content analysis and URL behavior analysis*, available at https://tinyurl.com/y7dkeeza; Gerke, M (2011) *Understanding Cybercrime: A Guide for Developing Countries*; CyberEdge Group (2020) *2020 Cyberthreat Defense Report*, available at https://tinyurl.com/y75uup6p

[209] SMS open rates are as high as 98% with an average response rate of 90 seconds. See Gartner (2016) Tap Into the Marketing Power of SMS, available at https://tinyurl.com/y7x93nf7; GSMA (2017*) RCS: A Formidable New Entrant to the Market for B2C Campaigns*, available at https://tinyurl.com/y7af3doo.

Purported wrong transfer scams are commonplace and thrive on impulse driven responses intended to bypass a customer's verification of the transaction.[210]

In the shadow of Safaricom announcing its independent funding efforts to fight the COVID-19 pandemic, fraudsters engaged in a pervasive and timely smishing scam. Text messages were sent to consumers about purported, non-existent Safaricom coronavirus offers such as cash relief assistance payments, free airtime and free Internet data offers. These campaigns induced victims to "verify" their customer status by texting their PIN numbers, passwords and account numbers to a number controlled by the fraudster.[211]

Industry experts and central banks we interviewed reported that while the pandemic had not been a source of inspiration for creating an entirely new types of smishing fraud, there was a noticeably increased volume of occurrence, especially smishing scams.

Exhibit 12: COVID-19 Smishing Scams

Related Studies. Only a handful of relevant smishing and vishing studies were identified in a developing country context and these few results provide a limited insight.[212] Respondents to a study of Indonesian students indicated that more were attacked using text messages (SMS 91%, voice 75%) which also yielded greater success rates (SMS 28%, voice 15%).[213] Twice as many women (24%) reported being previous victimized versus men (12%), with the most successful influence factor being the lure of a prize (24%). A small study of professionals in Ghana also yielded a greater volume of smishing attacks than vishing, with men being more susceptible to mobile-based vulnerability stemming from their risk-taking nature and abundance of comfort with online usage.[214] A 2018 consumer protection survey in Ghana (Ghana CP Survey) yielded relevant results relating to attack vectors and DFS scams, with participants reporting the following victimization rates: 29% by smishing and vishing attacks; 50% receiving transfer reversal requests with lower income persons being 19% more likely to be victimized by a scam.[215]

[210] Purported wrong transfer scams are covered in Section 3.3.1.1 Theft of Funds.
[211] Achuka, V (2020) *Subtle ways cybercriminals employ to con Kenyans*, available at https://tinyurl.com/y72s59ev; Kimuyu, H (2020) *Kenya: Safaricom: No, We Are Not Giving Away Free Relief Cash*, https://tinyurl.com/y97hla3t; Safaricom (2020) *Safaricom Commits KES200M to Fighting COVID-19 Pandemic*, available at https://tinyurl.com/ybm7gl88.
[212] As with the social engineering studies in Section 3.4, the participants, demographics, and testing environment are dissimilar and results should be observed with caution.
[213] Maulany, R and Yuyun, S (2017) *Comparative Analysis of Social Engineering Attack Based on SMS and Phone*.
[214] Yeboah-Boateng, EO and Amanor, PM (2014) *Phishing, SMiShing & Vishing: An Assessment of Threats Against Mobile Devices*, available at https://tinyurl.com/ybcpn28f; In a follow-up study of a local corporate bring-your-own-device policy (in which gender was not observed), most respondents considered unintentional disclosure of data and smishing attacks as medium and high security risks.
[215] Baur-Yazbeck, S and Frickenstien, J and Medine, D (2019) *Cyber Security in Financial Sector Developing: Challenges and potential solutions for financial inclusion.*

3.3.2.3 Vishing: Voice-Based Phishing

Vishing[216] uses the telephone voice channel to commit social engineering scams. In its simplest form, fraudsters may call random consumers directly, often posing as an authority to effectuate fee scams[217] and disclosure frauds.[218] Scalability is improved by solicitation of consumers (such as posing as a recognized authority) via SMS distribution containing a phone number for recipients to reply.[219] Robocalling may also be used, in conjunction with Voice Over Internet Protocol (VOIP), to "spoof"[220] originating telephone numbers, making the caller appear to have a familiar or local number.[221] Integrated voice recognition (IVR) systems can also be used to refine the efficiency of the fraud. Victims call a designated number and are prompted to navigate through a purported support system, eventually leaving messages as instructed which include PIN and other requested information to assist with the "verification" of their account.[222] As with smishing, very few relevant vishing studies related to developing countries were located.[223]

3.3.2.4 Pretexting / Impersonation

Pretexting attacks consist of creating a phony, contrived scenario to convince an unsuspecting person to trust the attacker and follow a requested directive, such as divulging sensitive and/or confidential information.[224] Common examples include a fraudster posing as an authority such as an MNO or DFSP support representative or outside consultant, which is illustrated by the SIM swap fraud example above in **Exhibit 11**. While pretexting may be categorized separately, it is often closely connected with a phishing, smishing or vishing attack. Pretexting is often distinguished from other types of mass attack methods, such as email phishing, in its more elaborate effort to convince victims beyond the ephemeral "cast and catch" nature of phishing attacks. Pretexting focuses predominantly on creating trust and building a

[216] Vishing attacks are covered in Section 3.3.2.3.
[217] The fraudster may pose as a recognized authority (an MNO, DFSP or bank employee) calling to inform customers they are prize winners of a current promotion but require an advance fee to deliver bicycles or scooters. GSMA handbook, Microsave (2014) *Survival of the Fittest: The Evolution of Frauds in Uganda's Mobile Money Market (Part-I).*
[218] Fraudsters may pose as tech support or help desk representatives to deceive customers into disclosing their PIN codes. Salahdine, F and Kabouch, N (2019) *Social Engineering Attacks: A Survey*.
[219] Kaspersky (2020) *What is Vishing?*, available at https://tinyurl.com/yb2c6bg6.
[220] Call spoofing occurs when an attacker intentionally places a false number to appear in the call receiver's caller identification display to conceal their identity and potential location. Federal Communications Commission (FCC) (2020) *Caller ID Spoofing*, available at https://tinyurl.com/gt6dzfm.
[221] Nguyen, N (2020) *Don't Click! Coronavirus Text and Phone Scams Are Designed to Trick You*, Wall Street Journal, available at https://tinyurl.com/y8p3q8rv.
[222] Salahdine, F and Kabouch, N (2019) *Social Engineering Attacks: A Survey*; Microsave (2014) *Survival of the Fittest: The Evolution of Frauds in Uganda's Mobile Money Market (Part-I).*
[223] A study of Nigerian university students examining phishing, vishing and pharming scams suggested that that: women may be more susceptible to phishing attacks than men; the type of vishing call can affect success rates; and that undergraduate students may be more familiar with phishing than vishing attacks.Ojugo, A and Otakore, O (2018) *Mitigating Social Engineering Menace in Nigerian* Universities, available at http://pubs.sciepub.com/jcsa/6/2/2/index.html; "Pharming" is the process of harvesting data from unsuspecting users directed to replica websites of legitimate service providers such as banks, MNOs, FSPs and government agencies.
[224] Salahdine, F and Kabouch, N (2019) *Social Engineering Attacks: A Survey*.

rapport with the victim to win their confidence, in contrast to preying on a momentary sense of urgency of the victim to respond that is characteristic of phishing attacks.[225]

3.4 Gender, Cybersecurity and Fraud Studies

Gender is one of several attributes, such as age and education, often included in studies exploring predictive behavior and attempts to identify susceptibility certain types of persons and their characteristics to social engineering frauds. This section concisely summarizes a small selection of the myriad of approaches observed in documented research efforts. While potentially useful for appreciating insight into relevant approaches taken in scientific and academic studies, most of the population demographics and key characteristics of these endeavors depart significantly in comparison to the women which comprise the subject of this paper. Limitations of these studies relating to application include sample sizes (often relatively small), population attributes (primarily developed countries, living in urban areas or university campuses),[226] testing designs and methodologies (questionnaires, simulations), technology used (predominantly smartphones with Internet access.) Application of these studies to women living in the poorest regions in SSA, SA and MENA who may use or are impacted by DFS may be substantially limited. Studies which have a greater connection to developing countries and potentially members of the BOP appear in Sections 3.3.2.2 and 3.3.2.3 which cover SMS-based and voice-based phishing.

3.4.1 Demographic Attributes: Gender, Age, Education

Several studies have examined several popular attributes alone and in tandem (gender, age, education, income) with some suggesting that women may generally be more susceptible than men to e-mail phishing attacks[227] and spoofing phishing attacks.[228] Other studies did not observe a meaningful correlation and suggested that additional and multiple factors may be present which can influence phishing susceptibility such as environmental (e.g. students might be more susceptible to phishing attacks than working professional although income and education might not be revealing characteristics.)[229]

---

[225] For a brief discussion of the trust rapport in contrast to the fear approach of phishing, see NordVPN (2019) *What is social engineering?*, available at https://nordvpn.com/blog/social-engineering/

[226] A sample of papers using university participants includes the following. Broadhurst, R and Skinner, K et. al. (2020) *Phishing and cybercrime risks in a university student community*; Ojugo, A and Otakore, O (2018) *Mitigating Social Engineering Menace in Nigerian Universities*; Sun, C-YS and Yu, S-J and Lin, SJ and Tseng, S-S (2016) *The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behavior and gender difference*, available at https://tinyurl.com/y92fw79m; Halevi T, Lewis J, and Memon N (2013) *Phishing, personality traits and Facebook*, available at https://arxiv.org/abs/1301.7643; Gratian, M and Bandi, S and Cukier, M et. al. (2017) *Correlating human traits and cyber security behavior intentions*, available at https://tinyurl.com/y8u3y3or; Dhamija, R and Tygar, JD and Hearst, M (2006) *Why Phishing Works*, available at https://tinyurl.com/ybndv378.

[227] Sheng, S, and Holbrook, M and Kumaraguru, P et. al. (2010) *Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions*, available at https://tinyurl.com/ybge5jkb; Darwish, A and El Zarka, A and Aloul, F (2012) *Towards Understanding Phishing Victims' Profile*, available at https://tinyurl.com/yahg77x7; McCormac A, Zwaans T, Parsons K et. al. (2017)

[228] Griffin, R (2018) *A Demographic Analysis to Determine User Vulnerability among Several Categories of Phishing Attacks*

[229] Griffin, R (2018) *A Demographic Analysis to Determine User Vulnerability among Several Categories of Phishing Attacks*, available at https://tinyurl.com/ycxa6rre; Parsons, K and Butavicius, et. al. (2019) *Predicting susceptibility to social influence*

Age is another popular demographic, also yielding a variety of results, sometimes antithetical: a negative correlation between age and phishing susceptibility (observing that younger users are likely more vulnerable and may be less risk-averse);[230] older women being most susceptible to spear phishing attacks including social engineering using "reciprocity" methods, while younger users were more susceptible to "scarcity/reward" attacks[231] (methods described in Section 3.3.1); a correlation of older age with lower phishing susceptibility resulting from greater experience/exposure to phishing and/or the Internet;[232] and studies reporting no correlation of any demographic factors to phishing susceptibility.[233]

Other studies observed gender, age and educational level, as well as prior phishing experience, yielding results suggesting a correlation may exist from a combination of these factors.[234] In social media and messaging contexts, phishing messages sent from students of the opposite sex resulted in greater phishing susceptibility of victims as well as slightly higher susceptibility of younger students.[235]

3.4.2 Personality and Character Traits

The "Big Five" personality traits, which comprise of openness, conscientiousness, extraversion, agreeableness and neuroticism (known by the acronym "OCEAN"), [236] have been used to explore

in phishing emails, available at https://tinyurl.com/y8t3ah6n; Butavicius, M and Parsons, K and Pattinson, M et. al. (2017) *Understanding susceptibility to phishing emails: assessing the impact of individual differences and culture*, available at https://tinyurl.com/ydgqoh2u; Flores, WR and Hom, H and Nohlberg, M and Ekstedt, M (2015*) Investigating personal determinants of phishing and the effect of national culture, available at* https://tinyurl.com/y8wn7wh9; Alseadoon, IM (2014) *The Impact of Users' Characteristics on their Ability to Detect Phishing Emails*, available at https://tinyurl.com/y9yfjoj9; (no significant correlation with gender found in 1,350 student phishing study in the US.) Diaz, A and Sherman, A and Joshi, A (2018) *Phishing in an Academic Community: A Study of User Susceptibility and Behavior*, available at https://tinyurl.com/y7sq5dc5.

[230] Alseadoon, IM (2014) *The Impact of Users' Characteristics on their Ability to Detect Phishing Emails*; Sheng, S, and Holbrook, M and Kumaraguru, P et. al. (2010) *Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions*.

[231] Oliveira, D and Rocha, H and Yang, H et. al. (2017) *Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing*, available at https://tinyurl.com/y8uy53kt.

[232] Older people with greater prior experience with and potential victimization by phishing might make them less susceptible. Gavett, B and Zhao, R and John, S et. al. (2017) *Phishing suspiciousness in older and younger adults: The role of executive functioning*, available at https://tinyurl.com/yd3k5kfk;

[233] Dhamija, R and Tygar, JD and Hearst, M (2006) *Why Phishing Works*.

[234] Gender may play a role in the following studies, in addition to age and income. Parsons, K and Butavicius, et. al. (2019) *Predicting susceptibility to social influence in phishing emails*; Cultural differences suggest different phishing susceptibility levels and while gender and age were not present, sample size was noted to be low and a potential factor of non-detection. Butavicius, M and Parsons, K and Pattinson, M et. al. (2017) *Understanding susceptibility to phishing emails: assessing the impact of individual differences and culture*; Gavett, B and Zhao, R and John, S et. al. (2017) *Phishing suspiciousness in older and younger adults: The role of executive functioning*; Gender and income did not factor although age, education and occupation presented significant differences. Griffin, R (2018) *A Demographic Analysis to Determine User Vulnerability among Several Categories of Phishing Attacks.*

[235] Jagatic, TN and Johnson, NA and Jakobsson, M and Menczer, F (2007) *Social Phishing*, available at https://dl.acm.org/doi/pdf/10.1145/1290958.1290968

[236] Several studies examined "The Big Five Personality Traits" – also known as the acronym "OCEAN" – comprising of openness, conscientiousness, extraversion, agreeableness and neuroticism. See Parrish, Jr. J L and Bailey, J L and Courtney, J

correlation of traits which may be useful in predicting cybersecurity skills and vulnerabilities in relation to gender. Studies have suggested that women with certain traits (such as extraversion) may exhibit weaker cybersecurity skills[237] and may be more susceptible (with the presence of neuroticism) to prize phishing fraud.[238] Opinions differ on the dominant trait correlating cybersecurity behavior and phishing susceptibility with the consideration that multiple factors may be interrelated.[239] Examination of literature and relevant studies also indicate varied results without a clear consensus of opinion.[240]

Character traits and influence factors were also examined,[241] attempting to profile characteristics most likely to indicate social engineering susceptibility, although no firm conclusion was observed to be drawn related to gender.[242] Some studies observed that people who are more trusting and obedient to authority tended to have higher degrees of phishing susceptibility.[243] Categories of phishing victims were also differentiated: the naïve who have low levels of suspicion; the doubtful who are aware of potential danger but don't make efforts to confirm suspicions; and risk takers who are aware of higher potential for problem but in disbelief of the likelihood of substantial consequences.[244] While these are helpful in understanding what type of DFS users may be more susceptible to certain types of social engineering frauds, it was not meaningfully and significantly insightful as to gender.

Women's confidence and self-efficacy[245] were also observed as potential indicators of greater phishing susceptibility than men, primarily in the context of student and organizational workplace settings covering

F (2009) *A Personality Based Model for Determining Susceptibility to Phishing Attacks*, available at http://swdsi.org/swdsi2009/Papers/9J05.pdf; Halevi, T and Lewis, J and Memon, N (2013) *Phishing, personality traits and Facebook*, available at https://arxiv.org/abs/1301.7643; Alseadoon, IM (2014) *The Impact of Users' Characteristics on their Ability to Detect Phishing Emails*.

[237] Extraversion was observed to be a predicting trait. Gratian, M and Bandi, S and Cukier, M et. al. (2017) *Correlating human traits and cyber security behavior intentions*.

[238] Neuroticism was observed to be a predicting trait. Halevi, T and Lewis, J and Memon, N (2013) *Phishing, personality traits and Facebook*.

[239] Studies have observed possible correlation of phishing susceptibility with females and neuroticism (Halevi 2012); openness and weaker privacy behavior (Pattinson 2012); and extraversion and perception of security risks (Rieulme and Roman 2014); Three factors were found to be correlated with high phishing susceptibility, being openness, extraversion and agreeableness. Alseadoon, IM (2014) *The Impact of Users' Characteristics on their Ability to Detect Phishing Emails*.

[240] Butavicius, M and Parsons, K and Pattinson, M et. al. (2017) *Understanding susceptibility to phishing emails: assessing the impact of individual differences and culture*.

[241] A list of DFS relevant influence factors can be found in Section 3.3.1 Social Engineering Methods and Techniques.

[242] Alexander, M (2016) *Methods for Understanding and Reducing Social Engineering Attacks*, available at https://www.sans.org/reading-room/whitepapers/engineering/paper/36972

[243] Agreeableness and extraversion were identified as potentially predicting greater phishing susceptibility. Cusack, B and Adedokun, K (2018) *The impact of personality traits on user's susceptibility to social engineering attacks*, available at https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1228&context=ism; Griffin, R (2018) *A Demographic Analysis to Determine User Vulnerability among Several Categories of Phishing Attacks*; Williams, E and Hinds, J and Joinson, A (2008) *Exploring susceptibility of phishing in the workplace*.

[244] Alseadoon, IM (2014) *The Impact of Users' Characteristics on their Ability to Detect Phishing Emails*.

[245] Self-efficacy is described as "whether a person believes that she can successfully execute the behavior required to produce the desired outcomes" with lower scores indicating a greater likelihood of phishing susceptibility. ENISA (2018) *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*, available at https://tinyurl.com/y99q8732

Internet e-mail and web phishing attempts.[246] These studies may be of limited applicability to the population of women examined in this paper and a brief insight into this topic is discussed in Section 4 Organizations and Cybersecurity Professionals.

3.4.3 National Culture

Several studies suggested a correlation may exist between national culture and cyber awareness, knowledge and behavior, as well as self-efficacy.[247] This finding was supplemented by another study which suggested that, in addition to national culture, beliefs and religion could also be factors which could reveal greater susceptibility or resistance to certain types of fraud.[248] A third found that user characteristics were also impacting on the ability to detect phishing e-mails.[249] This may support the notion that women in SA who are more impacted by greater social, cultural and religious extremes may inherently approach cybersecurity in a different manner than women in SSA.

3.5 Agents: Gender Representation and Fraud

DFS agents play a critically important role in the life cycle of a DFS consumer – they are the first point of contact for onboarding and first line of assistance for customer support.[250] As women in the BOP are generally more fearful about losing money and sensitive to negative news related to DFS,[251] the trust factor in agent relationships is of paramount importance. This section explores the role gender can play in the agent-customer relationship, examines agent selection by customers and identifies the most common agent-related frauds and cybersecurity related issues.

---

[246] (Women's self-efficacy and self-reported cyber behavior to be lower than men.) Anwar, M and He, W and Ah, I et. al. (2017) *Gender Difference and Employees Cybersecurity Behaviors*, available at https://tinyurl.com/y7a5ssms; (Female students' anti-phishing self-efficacy and anti-phishing behavior were found to be lower than males.) Sun, C-YS and Yu, S-J and Lin, SJ and Tseng, S-S (2016) *The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behavior and gender difference*; (Women were observed to have lower self-efficacy scores, potentially indicating greater phishing susceptibility, but they also generally possessed less technical experience) Sheng, S, and Holbrook, M and Kumaraguru, P et. al. (2010) Sun, C-YS and Yu, S-J and Lin, SJ and Tseng, S-S (2016) *The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behavior and gender difference*; Pattinson, M and Jerram, C and Parsons, K et. al. (2012) *Why do some people manage phishing emails better than others?*, available at https://tinyurl.com/ycxaag6a.

[247] Zwilling, M and Klien, G and Lesjak, D et. al. (2020) *Cyber Security Awareness, Knowledge and Behavior: A Comparative Study*, available at https://tinyurl.com/y7hwka46; Flores, WR and Hom, H and Nohlberg, M and Ekstedt, M (2015*) Investigating personal determinants of phishing and the effect of national culture.*

[248] Al-Hamar, M and Dawson, R and Guan, L (2010) *A culture of trust threatens security and privacy in Qatar*, available at https://ieeexplore.ieee.org/document/5578490

[249] Alseadoon, IM (2014) *The Impact of Users' Characteristics on their Ability to Detect Phishing Emails*; A fourth study found no gender influence existed but that sample size must likely be sufficiently large to perceive gender gaps. Butavicius, M and Parsons, K and Pattinson, M et. al. (2017) *Understanding susceptibility to phishing emails: assessing the impact of individual differences and culture*.

[250] For more on agent support and grievance resolution mechanisms, see Section 3.6.

[251] Tiwari, JA and Srivastava, Bhavana, Chatterjee, R et. al. (2019) *Gender Centrality of Mobile Financial Services in Bangladesh*; Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC. Interviews with practitioners, industry consultants, and field experts.

3.5.1 Gender Representation of Agents

The gender representation of DFS agents can vary significantly across regions. The overwhelming majority of the agent workforce in South Asia consists of men for reasons which can include the presence of historically patriarchal culture and religious and socio-economic influence, which may also include gender-based work barriers.[252] As of 2018, 99% of the agent workforce in Bangladesh was male.[253] A 2016 cross-regional agent study indicated representation as 100% male in Pakistan and 91% in India.[254] As of 2018, a larger percentage of women were reported to serve rural Indian areas, comprising of 71% female and 54% male. This experience is in contrast to those in several African countries which have greater gender diversity – Kenya (67%), Uganda (63%), Tanzania (47%), Zambia (46%) and Senegal (35%).[255]

The IFC Bangladesh Study represents some of the regional efforts made to improve gender representation.[256] Preferences of women were notably stronger favoring female agents in rural areas. Female perceptions were that women seemed to be more honest and trustworthy, provide more courteous service, and are more likely to maintain the privacy of data and confidentiality of transactions.[257] Bangladesh Bank noted that, from a sales perspective, women were generally more adept and handling and being received by multiple genders.

The most common complaint of women using DFS has been harassing calls from unknown men. The origin of how these men obtained their number is uncertain including: (i) shoulder surfers who lurk in the area to see/hear a woman/s phone number when communication with an agent; (ii) questionable agents who may share phone numbers of their female clients with other agents or persons.[258]

3.5.2 Agent Issues Through the Gender Lens

Agent Selection. As indicated earlier,[259] women are greatly influenced by family and peer group decisions, which includes choosing a network provider or which agent to use. Surveys in Bangladesh found that women were influenced to select an agent based on personal recommendations of family members, friends and knowledge of trust and reliability and sometimes to ensure physical safety.[260] Two Bangladesh studies

[252] For more on gender and social and cultural divides, see Section 2.3.
[253] Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC.
[254] Chatterjee, R and Khanna, M and Srivastava, B (2018) *India Needs More Women Business Correspondent Agents*, available at https://tinyurl.com/ydg7cep9
[255] Rousset, M and Bersudskaya, V (2016) *Building a Business Case for Women Agents*, available at https://tinyurl.com/yc449j79
[256] Bangladesh Bank (2018) *Women Mobile Financial Services Agent Recruitment Manual 2018*.
[257] Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC.
[258] Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC.
[259] See Section 2.3.1 Social, Cultural and Economic Divide and Exhibit 9.
[260] Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC. For more information on the issue of females and preferences for agent usage relevant to physical safety, see the following. Thakur, A and Sahoo, S and Barooah, P et. al. (2016) *Agency Banking: How Female Agents Make a Difference*, available at https://tinyurl.com/ycr28krw

reported a strong female preference for female agents, although this is perceived as a comfort issue and not trust which would inhibit or prevent usage.[261]

Women's DFS and Cybersecurity Awareness. Customer awareness of DFS fees, procedures and cybersecurity practices (such as PIN protection) was very low, especially among women. Research from the IFC Bangladesh Study found that only 10% of participants knew how to change their PINs and only 20% were aware of actual fees and costs of DFS services. As to actual fraud and loss: over 50% had lost money sending it to the wrong account (collectively suggesting likely reliance on agent assistance and greater susceptibility to fraud); 10% reported agent misuse of their PIN; and 7% reported agent misbehavior.[262]

Gender and Agent Fraud. As mentioned above, there is a general anecdotal perception that women agents may be more trustworthy than men.[263] In eastern Africa, males involved in DFS have been perceived to possess a higher incidence of fraud than females.[264] In contrast, the results of a 2020 study of rural Ghanaian villages suggested that 20% of mobile money transactions result in overcharges; female agents are 44% more likely to commit misconduct; male agents are 11% less likely to defraud male customers. It also found that where there is lower female empowerment there can be an incentive for women to engage in profit maximization when opportunity is presented.[265] Accordingly, the propensity for agent fraud and a potential relationship to gender, may vary for a variety of reasons as well as by region.

3.5.3 Agent Fraud and Misappropriation

In areas where literacy levels are low, agent assisted and OTC transactions are most common, such as in Bangladesh.[266] It is especially commonplace with women who possess lower literacy levels and who may not have DFS accounts or have substantial barriers to error-free usage.[267] These situations present the

[261] Tiwari, JA and Srivastava, Bhavana, Chatterjee, R et. al. (2019) *Gender Centrality of Mobile Financial Services in Bangladesh*; Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC.

[262] But while agent fraud was perceived as being a relatively high risk, few had reported actually being victims. Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC.

[263] See Section 3.5.1. See also Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC.

[264] Mudiri, JL (2012) *Fraud in Mobile Financial Services.*

[265] Annan, F (2020) *Gender and Financial Misconduct: A Field Experiment on Mobile Money*, available at https://tinyurl.com/yalvzxrl

[266] OTC is not encouraged in Sri Lanka and is more recently being discouraged in India. Riley, TA and Kylathunga, A (2018) *Bringing E-money to the Poor: Successes and Failures,* World Bank. While OTC is highly discouraged by the Bangladesh Bank, it is reported to occur often. Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh*, IFC.

[267] OTC activities are generally prohibited by regulation since the ultimate parties of the transaction are not recorded, but it is rarely enforced. Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh*, IFC.

highest risks of cybersecurity breaches and fraud. The follow represents common issues that DFS customers face when interacting with agents:[268]

- **OTC Fraud.** In one common OTC fraud, customers will give money to agents to conduct a transaction. But while the agent notifies the customer that the transaction has been completed, the customer does not receive a confirmation message and the party on the receiving end denies the transaction.[269] Agents may extract their own premiums from customers for providing OTC transactions. Customers may not be fully aware of the fees charged by agents nor that such practices are impermissible in various jurisdictions.[270]
- **Unauthorized use of customer's PIN.** As the customer PIN is the doorway into accessing customer accounts, it is a popular target – especially since customers may be trusting in agents for assistance and don't fully appreciate the nature of the circumstances and critical need for protection.[271] Unscrupulous agents may try to obtain a customer PIN for later unauthorized use or do so when freely given to them for assisted transactions, which is common.[272] They may also try to convince customers that a first transaction was unsuccessful and to repeat it a second time, ultimately providing the customer with funds for one transaction when two actually occurred.
- **Unauthorized use of customer transaction code.** An agent may inform a customer that the use of a transaction code for withdrawing funds was unsuccessful, only to be used later by an agent at another location.
- **Split Transactions.** Agents may pressure customers to split transactions into smaller amounts, such as not having sufficient cash on hand for withdrawals, so that they can generate greater commissions.
- **Imposition of illegal customer charges, tips, fees.** Agents may pressure customers to provide them with tips, charge them bogus or higher transaction fees, especially the case with illiterate customers.

3.6 Grievance, Resolution Mechanisms

Managing reputational risk of grievance resolution mechanisms in DFS is critically important. GRMs need to work reasonably well in order to maintain consumer and public confidence in the system. Once lost or diminished, efforts to regain confidence in the ecosystem becomes substantially more difficult. This is a challenging task in developing countries where victimized consumers are often held liable for losses related to electronic incidents, bear the burden of proving the loss and that the perpetration of the

[268] Mudiri, JL (2012) *Fraud in Mobile Financial Services*.
[269] Tiwari, JA and Srivastava, Bhavana, Chatterjee, R et. al. (2019) *Gender Centrality of Mobile Financial Services in Bangladesh*; Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC.
[270] Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh, IFC.*
[271] In the IFC Bangaldesh Study, 10% of respondents reported being victims. Barooah, P and Sahoo, S and Bhat, S and George, D (2018) C*losing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC.
[272] PIN sharing with agents for assistance is also common in Sri Lanka Riley, TA and Kylathunga, A (2018) *Bringing E-money to the Poor: Successes and Failures,* World Bank. It also occurs in Bangladesh. See Barooah, P and Sahoo, S and Bhat, S and George, D (2018) C*losing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC.

fraud was absent of negligence by the consumer.[273] As mentioned above in Section 2.3.2, women in the BOP tend to be extremely sensitive to negative news and loss of funds through DFS (fraud, mistake or otherwise).[274] In rural areas, women tend to be unaware of how to resolve issues that arise, most often turning to DFS agents, the first point of contact for DFS customers.[275]

Opinions shared during and surfacing from our research were consistent – that MNOs and DFSPs operations can operate reasonably well but, once a problem surfaces, solutions and remedies can be a laborious, time consuming process with minimal results to the great frustration of consumers.[276] The IFC Bangladesh Study found that agents may not be sufficiently trained or knowledgeable about resolution options or believe that certain issues are not their responsibility, leading to high frustration by rural customers who are left with unresolved problems and potentially written off.[277] 44% of respondents who faced issues opted not to file a complaint with 69% believing that resolution mechanisms were not in a reasonable timeframe to make pursuit worthwhile. From a gender perspective, women were considered to be better than men at handling complaints.[278]

While telephone support numbers may be available, these are often not known by or practically available to the average rural area DFS customer. Those customers who have limited literacy and who may not be tech savvy can encounter difficulty using IVR-based support systems and navigation. Long wait times are also reported. Since calls are not free, support calls can result in prohibitively expensive efforts with minimal results, if any.[279] Traveling to a local representative is also a suboptimal solution for rural area women, especially since closest available locations may be only in peri-urban areas. Women may need to wait for long time periods and make multiple return trips to remedy simple issues, which provides a disincentive to use and/or file complaints.

Exacerbating the experience is the likelihood of encountering men as support employees, especially challenging in more conservative and historically patriarchal regions such as Bangladesh, where over 99%

[273] Baur-Yazbeck, S and Frickenstien, J and Medine, D (2019) *Cyber Security in Financial Sector Developing: Challenges and potential solutions for financial inclusion.*
[274] *Bangladesh*, available at https://tinyurl.com/ycqxmv8t; Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC.
[275] Tiwari, JA and Srivastava, Bhavana, Chatterjee, R et. al. (2019) *Gender Centrality of Mobile Financial Services in Bangladesh*; Telephone resolution has consistently been referred to often as a time-consuming process but it does prevent the need for a significant effort to make a physical travel required by trips to local agent locations. Interviews with practitioners, industry consultants, and field experts.
[276] Interviews with practitioners, industry consultants, and field experts. See also Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC.
[277] Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC.
[278] World Bank (2018) *Women Mobile Financial Services Agent Training Manual: March 2018*, available at https://tinyurl.com/y8zmy8u9
[279]Interviews with practitioners, industry consultants, and field experts. Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC

of DFS agents are men.[280] Women's complaints on harassment and cyber related issues may not be taken seriously by those in authority and even legitimate concerns may be minimized. They may experience ridicule about their lower level of digital and financial literacy, blamed that an error or fraud is their fault at all levels – agents, GRM staff and even at home from male family members.[281]

As mentioned above, female victims of sexual harassment have a diminished faith in GRMs and the authorities themselves, predominantly seeking redress options through family and friends.[282] Women can exhibit tendencies to hesitate raising cyber harassment issues as filing police complaints in certain developing countries and regions, especially in SA.[283] The process can involve a torrent of questioning as well as the predictable embarrassment of going through the reporting process which will also leave embarrassing data with a male officer who may be untrustworthy and potentially distribute the information to others. Women in these areas often do not have faith in the authorities and find them perpetrators as well.[284] As such, GRMs can be ineffective for women and act as a disincentive to use DFS.

4 Organizations and Cybersecurity Professionals

This section briefly discusses gender issues on the service provider level, beginning with social engineering attacks on MNO and DFSP employees followed by a brief look gender representation in the African marketplace.

4.1 Internal Fraud

Insider threats within service providers can result from intentional fraud, such as an employee's sale of confidential customer information to third parties and/or collusion with external bad actors.[285] These attacks often yield the largest monetary frauds.[286] Service provider employees may also fall victim to unintentional insider threats or cyber breaches such as the result of social engineering, such as where fraudsters target vulnerable employees and deceive them into believing that they are in direct contact with

[280] Barooah, P and Sahoo, S and Bhat, S and George, D (2018) *Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh,* IFC.
[281] While the issue of women experience blame was reported in all regions, it was clearly more pronounced in SA and less so in Africa. Interviews with practitioners, industry consultants, and field experts. See also Section 2.3.2 Gender Imbalances, Women's Confidence and Sexual Harassment.
[282] Hassan, B and Unwin, T and Gardezi, A (2017) *Understanding the Darker Side of ICTs: Gender, Sexual Harassment, and Mobile Devices in Pakistan*; Interviews with practitioners, industry consultants, and field experts.
[283] See also Section 2.3.2 Gender Imbalances, Women's Confidence and Sexual Harassment.
[284] Interviews with practitioners, industry consultants, and field experts. NRD Cyber Security and Global Cyber Security Capacity Centre (2018) *Cybersecurity Capacity Review, Bangladesh August 2018*.
[285] There are 2 Microsave articles which talk about black market sales of this data which is later used to engage in SIM swaps.
[286] *Medine, D* and Makin, P (2018) *FAQs for regulators, supervisory authorities and digital financial services providers*, available at https://www.cgap.org/sites/default/files/event_documents/2018_10_15_Webinar-Presentation-Cyber-Security.PDF; In 2018, Airtel lost USD 6.7 million on its mobile money platform from cash control fraud perpetrated by employees. Olingo, A (2018*) Airtel Kenya lost $6.7 million in employee mobile money fraud*, available at https://www.theeastafrican.co.ke/business/Airtel-employee-mobile-money-fraud/2560-5175474-682fqwz/index.html; Morawczynski (2015) *Fraud in Uganda: How Millions Were Lost to Internal Collusion*, available at https://www.cgap.org/blog/fraud-uganda-how-millions-were-lost-internal-collusion

the customer who authorizes them to take an action harmful to the customer or unintentionally disclosing confidential customer information.[287]

4.2 Gender Representation Among Cybersecurity Professionals

It is not uncommon for information technology (IT) employees to possess multidisciplinary skills and be employed in various technology related roles which include cybersecurity responsibilities. Accordingly, the definition of what constitutes a cybersecurity professional or employee may vary between studies and surveys and represent variation in results.[288]

It has been estimated that, as of 2017, there were only 10,000 certified cybersecurity professionals in Africa of which more than one third were in Nigeria and Kenya.[289] Two recent worldwide studies have estimated the global gender representation of women in the cybersecurity workforce as 19%[290] and 24%,[291] but neither study appears to include Africa. Serianu estimated this number to be 10% in the private sector cybersecurity workforce in Kenya in 2018, with a notably higher presence in large private and public entities such as multinational corporations and consulting firms.[292] Our interviewees were consistent in sharing the opinion that these numbers could also be representative of many developing countries in Africa and South Asia.[293]

In addition to larger perceived gender gaps in the private sector within small to medium businesses, survey results and our interviewee observations were consistent as to other cybersecurity and IT industry characteristics. Female professionals often possessed substantial educational backgrounds, including post-graduate degrees in technology.[294]

---

[287] Software Engineering Institute (2014) *Unintentional Insider Threats: Social Engineering*, available at https://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_77459.pdf; Zwilling, M and Klien, G et. al. (2020) Cyber Security Awareness, Knowledge and Behavior: A Comparative Study.

[288] Frost and Sullivan's 2013 report, which cited an 11% female representation in the global cybersecurity workforce, has been very widely shared. However, its updated of report of 2019, which cites a much higher number, discusses the challenges of measurements such as women "who spend at least 25 percent of their time working on cybersecurity responsibilities." Morgan, S (2019) *(ISC)2 Aligns To Cybersecurity Ventures' Women In Cybersecurity Prediction Of 20 Percent*, Cybercrime Magazine, available at https://cybersecurityventures.com/women-in-cybersecurity-circa-2013/; (ISC)² (2019) *(ISC)² Cybersecurity Workforce Study: Women in Cybersecurity*, available at https://www.isc2.org/Research/Women-in-Cybersecurity; See also World Economic Forum (2020) Global Gender Gap Report 2020, available at http://www3.weforum.org/docs/WEF_GGGR_2020.pdf.

[289] Serianu (2017) *Demystifying Africa's Cyber Security Poverty Line*, available at https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf

[290] World Economic Forum (2020) Global Gender Gap Report 2020.

[291] (ISC)² (2019) *(ISC)² Cybersecurity Workforce Study: Women in Cybersecurity*.

[292] Serianu (2018) *Africa Cyber Security Gap (2018) – Kenya: Cyber Security Skills Gap*, available at https://www.serianu.com/downloads/KenyaCyberSecurityReport2018.pdf

[293] There is no known study which estimates the gender representation of cybersecurity professionals within MNOs and DFSPs although we were informed of a gender initiative within one African MNO.

[294] In addition to opinions of our interviewees, the 2019 (ISC)² survey reported that 52% of female and 44% of male respondents held post-graduate degrees. (ISC)² (2019) *(ISC)² Cybersecurity Workforce Study: Women in Cybersecurity.*

One interviewee specifically noted that there is a growing tendency to "have many women *around* technology but very few *actually within* it." Where women were visible in technology companies and divisions, they could be more concentrated in higher visibility non-technical roles, such as in sales, marketing and human resources related departments and positions.[295] Some interviewees noted that women also appeared more likely to serve in process, governance and compliance related roles in IT and cybersecurity than in those requiring hardcore technical skills such as penetration testing and coding.

As noted above in sections 2.2.3, 2.3.1 and 3.4.3, a sizeable gender gap exists in STEM school study on all levels and in professional pursuits. This a phenomenon that has been observed in many countries globally and potentially caused by a variety of factors which is outside the scope of this study.[296] The World Economic Forum's Global Gender Gap Report 2020 (GGGR) note that "investment in women's talent is insufficient" as pertaining to developing countries. Among a number of others echoing similar sentiments,[297] Serianu suggests that retention of women in the cybersecurity industry is challenging. As compared to men, women tend not to be: promoted at the same rate; obtain salary increases; as aggressive as men in applying for cybersecurity jobs; encouraged to enter the IT industry and can be influenced by perceived gender stereotypes which can define it as being more suitable for men.[298]

Behavioral Studies. Studies of the organizational workplace have suggested that when gender balance was not maintained, male dominated groups may be likely to engage in riskier behavior than risk averse females.[299] Others observed that women generally had lower self-efficacy scores, potentially indicating greater phishing susceptibility, but they also generally possessed less technical experience.[300]

[295] Microsave also mentioned this as did Laura and Evelyn at Safaricom in addition to human resources. Unwin, T (2020) *The attitudes and behaviours of men towards women and technology in Pakistan*, available at https://unwin.wordpress.com/2020/02/17/the-attitudes-and-behaviours-of-men-towards-women-and-technology-in-pakistan/

[296] For reference, see Wood, J (2020) *3 things to know about women in STEM*, WEF, available at https://www.weforum.org/agenda/2020/02/stem-gender-inequality-researchers-bias/; UNESCO (2020) STEM and Gender advancement (SAGA), available at https://bit.ly/3rdoLdY; Weeden, K and Gelbgiser, D and Morgan S (2020) *Pipeline Dreams: Occupational Plans and Gender Differences in STEM Major Persistence and Completion*, available at https://doi.org/10.1177/0038040720928484; See also studies of STEM capabilities by gender at OECD (2019) *Why don't more girls choose STEM careers?*, available at https://www.oecd.org/gender/data/why-dont-more-girls-choose-stem-careers.htm; Cimpian, J (2020) *Math-intensive fields have a gender problem: The men are worse at math*, Brookings, available at https://brook.gs/38gHmgu

[297] For more information, see UNESCO (2020) *Women in Science*, available at http://uis.unesco.org/en/topic/women-science

[298] Serianu (2018) *Africa Cyber Security Gap (2018) – Kenya: Cyber Security Skills Gap*. See also (ISC)² (2019) *(ISC)² Cybersecurity Workforce Study: Women in Cybersecurity*.

[299] CLTRe (2017) *Gender, Risk and Security*, available at https://get.clt.re/gender/

[300] Sheng, S, and Holbrook, M and Kumaraguru, P et. al. (2010) Sun, C-YS and Yu, S-J and Lin, SJ and Tseng, S-S (2016) *The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behavior and gender difference*; Pattinson, M and Jerram, C and Parsons, K et. al. (2012) *Why do some people manage phishing emails better than others?*; Anwar, M and He, W and Ah, I et. al. (2017) *Gender Difference and Employees Cybersecurity Behaviors*.

5 Conclusions

This study conducted a high-level exploration of two regions and several countries examining the possibility of identifying correlation of gender, cybersecurity, fraud and DFS in developing countries. Our conclusions are as follows:

Data and information gathering.

- We observed that a paucity of current, publicly accessible cybersecurity and consumer fraud related data is visible from our survey of developing countries. Available cybersecurity data – including within national reports including from CERTS – tended to be broad, unsegmented, lacking significant detail and rarely gender-disaggregated. Limited supply side information is available, such as agent representation and product and services consumption by gender. Several of our interviewees suggested that a greater priority needs to be placed on women as a substantial consumer base as well as possessing special needs and attention as a result of the impact of gender divides.

Overall conclusions and findings.

- Our review of data and interviews with consultants in the field suggests that substantial social, cultural and educational gender divides still exist, more pronounced in several countries studied in South Asia.
- Basic and feature phones appear to be still predominantly in use among women in developing countries, especially in rural areas. Adult women are more likely to lag behind men regarding phone ownership, handset type and upgrades to superior equipment. Evidence suggests that smartphones are gaining popularity, more quickly among men and the youth, but still not predominant in rural areas.
- DFS onboarding remains a greater challenge for women and thus may limit their incentive to use DFS and technology. Challenges include traditional gender roles in the household; distance required to travel from the home to acquire national identification; legal barriers women still face in some countries; and social, cultural and workplace hurdles and challenges.
- The presence of male dominant gender representation can impact women's behavior and attitudes towards DFS and technology. Representation is still heavily skewed towards men in several countries, more noticeably in South Asia such as with regard to agents, GRM employees and law enforcement.

Cybersecurity specific observations.

- Cybersecurity incidents and social engineering fraud have grown substantially and present a predominant problem in developing countries. Fraudsters capitalize on low priority placed on cybersecurity at the service provider level, weak legal and regulatory protections of consumers, and generally lower levels of digital literacy, cyber awareness and hygiene in Africa and South Asia.
- The impact of gender divides in developing countries can lead to limited levels of exposure to and experience with technology, resulting in lower cyber awareness and hygiene among women.
- Peer knowledge networks are critically important for capacity building, where novices can more easily and readily learn about fraud prevention and technology best practices for cyber awareness, hygiene

and security. Answers to questions are often through conversation, on a level of understanding appreciated by participants and may cover timely information and warnings concerning new scams and frauds. These are especially important to women in DFS countries, who have limited capacity at time of onboarding by MNOs and DFSPs and, subsequently, are rarely supplemented effectively.

- Women's social, cultural, legal and workplace barriers can limit their mobility and access to meeting places such as cafes, social events, the marketplace and virtual spaces, where a substantial amount of relevant cybersecurity, cybercrime and DFS education takes place. These places also foster growth and strength of critically important peer knowledge networks.
- While the representation of women in the cybersecurity industry is increasing, women's roles may still be predominantly in positions requiring less technical skills.
- Academic and scientific studies exploring the relationship of gender and social engineering and cybersecurity practices vary greatly in scope and coverage. Our observations perceived that, to a notable degree, no clear consensus of opinion exists among these studies. The testing conditions, populations and focus of most of these studies were often at a substantial variance with those contemplated in and relevant to this paper.

6 Recommendations

- The increased penetration of ICT and DFS in developing countries should mandate greater initiatives and efforts at capturing and sharing ICT, DFS and cybersecurity related data. Attention should be given to prioritize the capture and sharing of gender disaggregated data at data collection points as a general practice. Industry may serve as a driver for this initiative.
- Concerted efforts should be made to raise the level of cyber awareness and hygiene in DFS countries. These include those made by MNOs and DFSPs at time of onboarding as well as subsequently. Industry and government should supplement these efforts, which also needs to incorporate an initiative at the grassroots level in order to be effective.
- Continued reduction of social and cultural gender gaps may meaningfully reduce DFS and technology divides. Women's confidence and capacity levels in using DFS and ICT are an important driver towards their adoption and use and investment in learning cybersecurity best practices.
- Regions which exhibit substantial gender representation divides among DFS related personnel, such as agents and GRM representatives, should consider the initiatives of and efforts made by the Bank of Bangladesh and others, such as female agent recruitment and training programs.
- Greater emphasis and efforts should be made to encourage women to seek cyber and consumer fraud related assistance and reporting, which could increase women's confidence in the system. Examples include a cost-free hot line or reporting pipeline and/or text messaging, which may make women in rural areas less reluctant to seek assistance when confronted with ICT or DFS related knowledge gaps or when they believe they have been or might be exposed to fraud.
- Efforts should be made at improved tracking of smartphone adoption and usage. While the data indicates increasing smartphone penetration, research also revealed that what is considered a smartphone can noticeably lag behind the curve in terms of quality and performance. Network

coverage and power/charging availability also create challenges, but the time would appear ripe to prioritize the creation and capture of a richer data set which would include gender disaggregation, security and usage trends.

- Women's encouragement and participation in STEM study and careers should be an important priority in developing countries. In rural areas, additional efforts should be made to increase basic financial and digital literacy levels.
- Policy makers, regulators and financial services providers should consider increasing efforts towards an inclusive approach of "gender centrality" to ensure that gender-specific needs are addressed. This would appear to be of greater importance as it relates to ICT and mobile communications, an area where there is a notable gender divide which is more pronounced in rural areas. [301]

Trust in financial systems and the technology which drives the process is the mainstay of user adoption. Yet we have found that there are significant gender gaps relating to access to information, education, and ICT which lead to lower levels of digital capacity, technical literacy and, logically, reduced fraud and cyber awareness. The distinct lack of quantitative and qualitative research on cybersecurity as well as gender differences – such as overall level of cyber awareness and hygiene, susceptibility to fraud, social engineering and cyber-attacks – compels the need for additional focus, funding and attention to address this important issue by academic institutions, donor communities and think tanks.

[301] "The first step in this direction would be to recognize that women and men have different needs, aspirations, perceptions, and behaviors, which are influenced by prevailing gender norms and inequalities. The next step would be to apply this understanding to the design, delivery, and provision of financial services. By doing so, gender aspects would become a central element of the provision of financial services to achieve gender equitable outcomes." Tiwari, A and Srivastava, B and Rangaswami, S (2018) *A comprehensive framework for gender centrality in financial services*.