

MODERATING EFFECT OF CYBERSECURITY CULTURE ON THE RELATIONSHIP BETWEEN DIGITAL FORENSIC INVESTIGATION COMPETENCE AND CYBER-FRAUD DETECTION EFFECTIVENESS AMONG FINTECH FIRMS IN NIGERIA

Ganiyu A. Mustapha ganiyumustapha84@gmail.com

Adegbemi Titilayo Adesola teeboyad@gmail.com

Oriloye Muiyiwa James funshlaw@gmail.com

Samuel Ogboloja ogbolojasamuel@gmail.com

ANAN University, Kwall, Jos, Nigeria

Abstract

Nigerian financial technology firms have expanded their forensic tooling, analyst teams, and investigative routines, yet fraud losses have continued to climb, exposing a gap between the capability firms hold and the detection they achieve. This study examined the moderating effect of cybersecurity culture on the relationship between digital forensic investigation competence and cyber-fraud detection effectiveness among FinTech firms in Nigeria. From an accessible population of 140 licensed FinTech firms supervised by the Central Bank of Nigeria and affiliated with the FinTech Association of Nigeria, each represented by a principal officer responsible for cyber-fraud and digital-forensic functions, a sample of 103 was drawn using the Taro Yamane formula and purposive selection. Primary data from a structured five-point Likert questionnaire were analysed through partial least squares structural equation modelling (PLS-SEM) in SmartPLS. The measurement model satisfied indicator reliability, internal consistency, and convergent validity, and discriminant validity held under both the Fornell-Larcker criterion and the HTMT ratio. Digital evidence analysis capability ($\beta=0.284$, $p < 0.001$), digital forensic tools sophistication ($\beta=0.221$, $p < 0.01$), and digital forensic personnel expertise ($\beta=0.318$, $p < 0.001$) each raised detection effectiveness, with personnel expertise the strongest antecedent. Cybersecurity culture strengthened the competence-to-detection relationship as a moderator ($\beta = 0.149$, $p < 0.05$) and acted directly on detection ($\beta=0.196$, $p < 0.05$). Forensic investment pays its fullest dividend only where security culture is strong enough to put it to work. The study recommends targeted development of forensic personnel, deliberate cultivation of security culture, and continual renewal of the forensic toolset.

Keywords: cyber-fraud detection; digital forensic investigation competence; digital evidence analysis; forensic tools; forensic personnel expertise; cybersecurity culture; FinTech; Nigeria.

Word count = 250 words

Introduction

Digital finance has rearranged not only how value moves but also the economics of defrauding it. Where settlement once took days, funds now clear in seconds and across borders, and the interval in which an illicit transaction can be intercepted has

collapsed accordingly. Detection, rather than after-the-event recovery, has therefore become the decisive line of defence, and the accuracy and speed with which a provider surfaces fraud now stand among the clearest signals of its trustworthiness (Akinbowale et al., 2023;

Daraojimba et al., 2024). Static, rule-based monitoring that once coped with predictable schemes strains against adversaries who have industrialised their methods, and the response internationally has tilted towards forensic, intelligence-led investigation able to reconstruct how a fraud unfolded and to establish it to an evidentiary standard.

These pressures bear down hardest on developing economies, where digital finance has outgrown the institutions meant to supervise it. The swift uptake of mobile money, agency banking, and application-based payments has widened financial access, but the forensic scaffolding that should accompany it, namely skilled investigators, capable analytic tools, and disciplined organisational routines, has lagged (Aziz & Andriansyah, 2023; Dubey et al., 2023). In markets where inclusion rests largely on public trust, a single conspicuous detection failure can shake confidence out of proportion to its direct cost, which reframes the reliability of fraud detection as a development question rather than a narrowly technical one.

Africa displays this imbalance in sharp relief. The continent's fintech boom has arrived alongside patchy incident reporting and shallow investigative capacity, so that similar technological outlays deliver strong detection in one institution and weak detection in another (Awodiran et al., 2023; Olaiya et al., 2024). Such variance is difficult to explain by tooling alone; it points instead to how investigators work and to the organisational conditions that

shape their conduct (Da Veiga et al., 2020; Uchendu et al., 2021).

Nigeria brings this tension to its fullest expression. As the largest fintech market on the continent, host to more than four hundred licensed financial technology firms and to roughly a quarter of Africa's fintech companies, it concentrates both the opportunity and the exposure of digital finance. The Nigeria Inter-Bank Settlement System placed fraud losses across financial institutions at about N52.26 billion in 2024, close to triple the N17.67 billion recorded a year earlier, at a time when the value of electronic payments crossed the one-quadrillion-naira mark (Nigeria Inter-Bank Settlement System, 2025). A near-tripling of losses within twelve months, set against record transaction volumes, is telling: the machinery of payment has outrun the machinery of protection.

The Nigerian authorities have not stood still. The Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act of 2024 tightened the duty of financial institutions to detect, report, and preserve evidence of cyber-enabled fraud, and the Central Bank of Nigeria has linked prudential expectations to the soundness of institutions' control environments (Federal Republic of Nigeria, 2024; Central Bank of Nigeria, 2024). That regulatory push has drawn fintechs into forensic analytics, incident-response capability, and specialist recruitment. Losses have nonetheless persisted, and it is this stubbornness that motivates the present enquiry: the capability has been bought, yet the detection it promised remains inconsistent.

The fintech sector is the natural place to interrogate that inconsistency. Fintech firms sit at the frontline of digital-financial fraud, carry the transaction volumes most attractive to offenders, and answer directly to the Central Bank of Nigeria and to the coordinating structures of the FinTech Association of Nigeria. They also house the dedicated forensic functions, the analysts, the toolsets, and the investigative processes, whose effectiveness is at issue here. Focusing on regulated fintechs isolates the organisational setting in which forensic competence is at once most developed and most severely tested.

The outcome this study seeks to explain, cyber-fraud detection effectiveness, concerns how accurately and promptly a firm identifies fraudulent activity while keeping false alarms low enough not to degrade legitimate service (Awodiran et al., 2023; Micah et al., 2023). Its central antecedent, digital forensic investigation competence, is treated not as a single trait but as a bundle of three separable capabilities: the analytical handling of digital evidence, the sophistication of the forensic toolset, and the expertise of forensic personnel. Distinguishing them matters because firms can resource each independently, and Nigerian fintechs differ markedly in which they have chosen to prioritise.

What turns these capabilities into realised detection is far less obvious. A firm may retain certified investigators and license advanced analytics yet still overlook fraud when its people regard security as another department's concern, quietly set aside inconvenient alerts, or bypass controls

under commercial pressure. Cybersecurity culture, understood as the shared norms and routines that make security a collective practice rather than a compliance ritual (Da Veiga et al., 2020; Uchendu et al., 2021), plausibly determines whether forensic competence is fully exploited. The uneven returns to forensic investment observed in Nigerian and comparable settings (Akinbowale et al., 2021; Olaiya et al., 2024) are consistent with exactly this kind of conditioning mechanism.

Three gaps persist despite an expanding Nigerian literature on forensic accounting and cyber fraud. Empirically, no study has yet tested, with primary data and variance-based structural equation modelling, whether cybersecurity culture moderates the link between forensic investigation competence and detection effectiveness in Nigerian fintechs. Conceptually, forensic competence has usually been handled as a single block rather than unpacked into its evidence, tooling, and personnel elements. Contextually, the available evidence rests largely on banks and accounting professionals rather than on the fintech security specialists who now occupy the centre of the detection problem (Afriyie et al., 2023; Awodiran et al., 2023; Micah et al., 2023).

Resolving these gaps carries practical consequence. Should detection return indeed hinge on culture, then training budgets, recruitment, and supervisory benchmarks ought to target the organisational conditions that release forensic capability, not the capability in isolation. On that basis, this study examines the moderating effect of

cybersecurity culture on the relationship between digital forensic investigation competence and cyber-fraud detection effectiveness among fintech firms in Nigeria. Its specific objectives are to:

- i. examine the effect of digital evidence analysis capability on cyber-fraud detection effectiveness among FinTech firms in Nigeria;
- ii. assess the effect of digital forensic tools sophistication on cyber-fraud detection effectiveness among FinTech firms in Nigeria;
- iii. evaluate the effect of digital forensic personnel expertise on cyber-fraud detection effectiveness among FinTech firms in Nigeria; and
- iv. examine the moderating effect of cybersecurity culture on the relationship between digital forensic investigation competence and cyber-fraud detection effectiveness among FinTech firms in Nigeria.

The corresponding null hypotheses are developed and stated within the conceptual review that follows. Beyond its scholarly contribution, the study speaks to a live

policy choice for fintech boards, the Central Bank of Nigeria, and the FinTech Association of Nigeria, namely whether cybersecurity culture can serve as a practical lever for turning forensic investigation into genuine detection capability across Nigeria's digital-finance sector.

Literature Review and Hypothesis Development

Conceptual Framework

Figure 1 sets out the relationships the study tests. Three dimensions of digital forensic investigation competence, namely evidence analysis capability, tools sophistication, and personnel expertise, are modelled as direct antecedents of cyber-fraud detection effectiveness, while cybersecurity culture is positioned as a moderator that conditions the strength of each of those paths. The framework is deliberately additive on the competence side and interactive on the culture side, reflecting the study's contention that resources and the conditions for using them are analytically distinct.

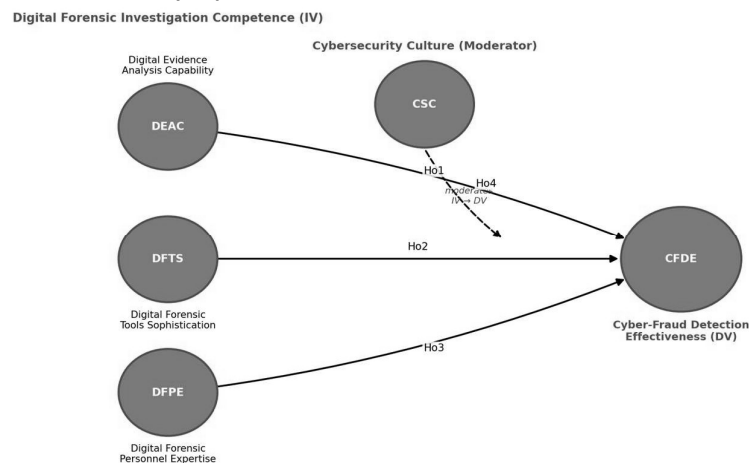


Figure 1: Conceptual Framework of the Study Cyber-Fraud Detection Effectiveness

Detection effectiveness is best read as an outcome rather than an activity: the extent to which a firm accurately and early catches fraudulent transactions, with evidence robust enough to support action, without smothering genuine customers under false alerts (Awodiran et al., 2023; Micah et al., 2023). Four observable qualities capture it in the Nigerian fintech setting, namely the accuracy of identification, the timeliness of response, the evidentiary quality of investigative output, and the containment of false positives (Afriyie et al., 2023). The construct is sensitive to how mature the forensic function is and to how faithfully the investigative process is followed (Akinbowale et al., 2023; Dubey et al., 2023), and it is operationalised here through respondents' assessments of those four qualities.

Digital Evidence Analysis Capability and Detection Effectiveness

The first competence dimension concerns what a firm can do with digital traces once fraud is suspected: how well it acquires, preserves, and interrogates logs and artefacts so that raw data becomes an admissible investigative signal. Analytical capability is the point at which suspicion either hardens into a detectable pattern or dissipates, since only carefully handled evidence supports a defensible conclusion about wrongdoing (Dubey et al., 2023; Awodiran et al., 2023). Firms that maintain disciplined acquisition, an unbroken chain of custody, and rigorous analysis tend to surface anomalies sooner and to carry them further as evidence.

The empirical record is consistent on this point. Awodiran et al. (2023) reported that digital forensic accounting techniques materially improved the detection of cyber fraud among Nigerian financial entities, and Dubey et al. (2023) showed that advances in forensic analysis raise the reliability of investigative findings. Read alongside Afriyie et al. (2023), for whom forensic capability is decisive for both detecting and preventing fraud, and Akinbowale et al. (2020), who linked structured techniques to the identification of economic crime, these studies converge on evidence analysis as a primary route to detection. The first hypothesis is accordingly stated in null form: Ho1: Digital evidence analysis capability has no significant effect on cyber-fraud detection effectiveness among FinTech firms in Nigeria.

Digital Forensic Tools Sophistication and Detection Effectiveness

The second dimension shifts attention from analytical practice to the instruments that enable it: the range, currency, automation, and interoperability of the technologies a firm deploys against fraud. Tooling earns its place where transaction volumes and adversarial ingenuity exceed what human review can track, because advanced and well-integrated systems expose correlations that manual inspection would miss (Dubey et al., 2023; Aziz & Andriansyah, 2023). A capable toolset narrows the blind spots by automating the search for anomalies and by joining signals that would otherwise sit in separate silos.

Evidence from several strands supports the link. Dubey et al. (2023) found that the sophistication and integration of forensic tools govern the speed and accuracy of investigation, while Aziz and Andriansyah (2023) demonstrated that artificial-intelligence-driven analytics markedly improve fraud prevention and detection in banking. Akinbowale et al. (2023) attributed measurable gains in fraud-risk mitigation to advanced forensic techniques, and Olaiya et al. (2024) placed the technology layer at the heart of safeguarding financial data in fintech. Synthesising these findings yields the second null hypothesis: Ho2: Digital forensic tools sophistication has no significant effect on cyber-fraud detection effectiveness among FinTech firms in Nigeria.

Digital Forensic Personnel Expertise and Detection Effectiveness

Tools and evidence are inert without the people who wield them, which brings the third dimension into focus: the certification, experience, and analytical judgement of forensic staff. Expertise is decisive precisely where cases are ambiguous, because a skilled investigator distinguishes signal from noise, resists both omission and over-flagging, and translates tool output into conclusions that will withstand scrutiny (Afriyie et al., 2023; Micah et al., 2023). Where such proficiency is abundant, the latent value of evidence and tooling is realised; where it is scarce, the same resources sit underused.

The literature treats investigator competence as pivotal. Afriyie et al. (2023) established the centrality of forensic

accountants' knowledge to effective detection and prevention, and Micah et al. (2023) traced how the shifting skill demands of digital forensics shape the effectiveness of Nigerian practitioners. Akinbowale et al. (2021) showed that pairing forensic expertise with management control strengthens the response to cyberfraud, and Daraojimba et al. (2024) identified investigator competence as a leading determinant of digital financial fraud prevention. These accounts justify the third null hypothesis: Ho3: Digital forensic personnel expertise has no significant effect on cyber-fraud detection effectiveness among FinTech firms in Nigeria.

Cybersecurity Culture as Moderator

The three competence dimensions describe what a firm can do; cybersecurity culture describes whether it will. Culture here denotes the shared assumptions, norms, and routines that make security a collective behaviour rather than a box-ticking exercise (Da Veiga et al., 2020; Uchendu et al., 2021). Its moderating role follows from a simple observation: a well-equipped forensic function returns little where staff circumvent controls, sit on awkward alerts, or treat awareness training as theatre. Culture, on this reasoning, is the condition under which competence is either fully mobilised or quietly wasted.

Da Veiga et al. (2020) established that a clearly defined information-security culture strengthens secure behaviour and organisational resilience, and Uchendu et al. (2021) showed that maturing such a culture is what converts security investment into protective practice. Olaiya

et al. (2024) placed human and cultural factors at the core of safeguarding financial data in fintech, while Akinbowale et al. (2021) demonstrated that the organisational control environment conditions how effectively forensic functions counter cyberfraud. Taken together, these studies imply that culture does not merely add to detection but shapes the payoff to forensic competence, which is expressed as the fourth null hypothesis: Ho4: Cybersecurity culture has no significant moderating effect on the relationship between digital forensic investigation competence and cyber-fraud detection effectiveness among FinTech firms in Nigeria.

Theoretical Framework

The study draws its primary logic from the resource-based view, first articulated by Wernerfelt (1984) and formalised by Barney (1991), which holds that durable advantage flows from resources that are valuable, rare, difficult to imitate, and organised for use. Forensic investigation competence fits this description closely: the analytical capability, tooling, and expertise a fintech assembles are firm-specific, costly for rivals to replicate, and directly bound up with the ability to detect fraud (Bharadwaj, 2000; Akinbowale et al., 2023). The final clause of the resource-based view, that resources yield advantage only when the firm is organised to exploit them, supplies the theoretical warrant for treating cybersecurity culture as a moderator rather than a mere covariate: culture is the organising condition that decides whether forensic resources are converted into detection or left dormant.

The technology-organisation-environment framework of Tornatzky and Fleischer (1990) complements this account by situating capability within three settings. It reads tools sophistication as the technological setting, personnel expertise and culture as the organisational setting, and the regulatory and threat landscape, including oversight by the Central Bank of Nigeria and the deteriorating fraud environment charted by the Nigeria Inter-Bank Settlement System (2025), as the environmental setting. Where the resource-based view explains why forensic resources should raise detection, the technology-organisation-environment framework explains why identical resources perform unevenly across firms, and the two together provide a coherent foundation for the moderated model examined below.

Methodology

A cross-sectional survey design within a positivist frame was adopted, on the premise that the relationships among forensic competence, cybersecurity culture, and detection effectiveness can be measured and tested through systematic observation. The population comprised licensed financial technology firms operating in Nigeria as at January 2026, specifically those under the supervision of the Central Bank of Nigeria and affiliated with the FinTech Association of Nigeria, each represented by a principal officer whose remit covers cyber-fraud and digital-forensic functions. Eligible respondents held roles such as chief information-security officer, information-security or IT manager, fraud-risk manager, digital-forensic analyst, internal or IT auditor, and

compliance or risk officer. Concentrating on regulated fintechs is defensible on three counts: these firms run the full complement of forensic and detection technologies the constructs describe; they bear the supervisory duties under which detection is judged; and a workable frame of identifiable principal respondents is reachable through industry-association structures. On that basis, the accessible population was 140 firms. Because the constructs demand informed judgement rather than lay opinion, purposive sampling was used to restrict participation to officers with direct oversight of detection processes, an approach suited to settings where specialised knowledge, not demographic spread, governs the quality of response. Sample size was fixed with the Taro Yamane (1967) formula:

$$n = N / (1 + N(e)^2)$$

With $N = 140$ and a 5% margin of error ($e = 0.05$), the calculation gives $n = 140 / [1 + 140 (0.05)^2] = 140 / (1 + 0.35) = 140 / 1.35$, which rounds to 103. A sample of 103 sits comfortably above the thresholds implied by the inverse-square-root and ten-times rules for a model with this number of structural paths (Hair et al., 2022).

Instrument and Data Collection

Data were gathered with a structured questionnaire built around a five-point Likert scale (1 = strongly disagree to 5 = strongly agree) and arranged in six parts: respondent demographics (Section A) and the five constructs in turn, namely digital evidence analysis capability, digital forensic tools sophistication, digital forensic personnel expertise, cybersecurity culture, and cyber-fraud detection effectiveness (Sections B to F). Items were adapted from validated prior instruments (Da Veiga et al., 2020; Uchendu et al., 2021; Ogwiji & Lasisi, 2022) and reworded for the Nigerian fintech context. Two academics in forensic accounting and information security and two practising digital-forensic professionals confirmed content and face validity, and a pilot exercise verified item clarity before full fieldwork. Cronbach's Alpha (threshold $\alpha \geq 0.70$) confirmed reliability. To limit non-response, 120 questionnaires were distributed; 108 were returned and 103 were complete and usable, a usable response rate of 85.8%. Ethical clearance, informed consent, and respondent anonymity were observed throughout. Table 1 summarises the constructs, their measurement, and their sources.

Table 1: Variables and Measurement

Variable	Type	Measurement Scale	Source
Cyber-Fraud Detection Effectiveness (CFDE)	Dependent	Accuracy, timeliness, evidentiary quality, false-positive control; 5-pt Likert (5 items)	Awodiran et al. (2023); Micah et al. (2023)
Digital Evidence Analysis Capability (DEAC)	Independent	Acquisition, preservation, integrity, analysis maturity; 5-pt Likert (4 items)	Dubey et al. (2023)
Digital Forensic Tools Sophistication (DFTS)	Independent	Tool breadth, currency, automation, integration; 5-pt Likert (4 items)	Akinbowale et al. (2023)
Digital Forensic Personnel Expertise (DFPE)	Independent	Certification, experience, analytic proficiency; 5-pt Likert (4 items)	Afriyie et al. (2023)
Cybersecurity Culture (CSC)	Moderating	Awareness, leadership commitment, reporting norms, shared responsibility; 5-pt Likert (4 items)	Da Veiga et al. (2020); Uchendu et al. (2021)

Source: Authors' compilation, 2026.

Method of Data Analysis

Analysis used partial least squares structural equation modelling (PLS-SEM) in SmartPLS, chosen because it handles reflectively measured latent constructs, tolerates modest samples and non-normal data, and lends itself to interaction modelling (Hair et al., 2022; Sarstedt et al., 2022). Estimation proceeded in the conventional two stages. The measurement model was first assessed for indicator reliability, internal consistency, convergent validity, and discriminant validity using the Fornell and Larcker criterion and the HTMT ratio; the structural model was then evaluated for explanatory and predictive power (R^2 , Q^2 , and f^2) with significance established by bootstrapping across 5,000 subsamples. The moderating

effect was captured through the product-indicator (interaction-term) approach, and common-method concerns were addressed following the full collinearity check recommended by Kock (2015) and the discriminant-validity procedure of Henseler et al. (2015).

Model Specification

The model treats cyber-fraud detection effectiveness as the dependent construct; digital evidence analysis capability, digital forensic tools sophistication, and digital forensic personnel expertise as the independent constructs that jointly form digital forensic investigation competence; and cybersecurity culture as the moderator. The structural equation is written as:

$$CFDE_i = \beta_0 + \beta_1 DEAC_i + \beta_2 DFTS_i + \beta_3 DFPE_i + \beta_4 CSC_i + \beta_5 (DFIC_i \times CSC_i) + \varepsilon_i$$

where CFDE is cyber-fraud detection effectiveness; DEAC, DFTS, and DFPE are the three competence dimensions; CSC is cybersecurity culture; (DFIC $\times$ CSC) is the interaction term carrying the moderating effect, with DFIC the composite competence score; β_0 is the intercept; β_1 to β_5 are path coefficients; and ε is the error term. Theory and the hypotheses lead to the a priori expectations $\beta_1, \beta_2, \beta_3 > 0$ for the direct effects of competence, $\beta_4 > 0$ for the direct effect of culture, and $\beta_5 > 0$ for a positive moderation in which stronger culture steepens the competence-to-detection relationship. Three figures express the model: the conceptual framework at Figure 1, the estimated measurement and structural model at Figure 2, and the bootstrapped path model at Figure 3.

Results and Discussion

Response Rate and Respondent Profile

Of the 120 questionnaires distributed, 108 were returned, and 103 proved complete and usable, a usable response rate of 85.8% that sits well above the level ordinarily regarded as adequate for survey inference. Table 2 profiles the 103 respondents. Men made up the majority at 62.1%, in keeping with the composition of the forensic and security cadre, and the 30-to-39 age band was the largest at 45.6%, marking a mid-career sample. Educationally, the group was strong: half (50.5%) held a postgraduate qualification, and a further 30.1% held an HND or bachelor's degree. Roles spread across internal and IT auditors (23.3%), fraud-risk managers (20.4%), compliance and risk officers (17.5%), information-security officers (16.5%), digital-forensic analysts (14.6%), and IT managers (7.8%). More than three-quarters (78.6%) had at least five years of experience, which lends weight to their assessments.

Table 2: Demographic Profile of Respondents

Variable	Category	Frequency	Percentage (%)
Gender	Male	64	62.1
	Female	39	37.9
Age (years)	Below 30	18	17.5
	30 to 39	47	45.6
	40 to 49	27	26.2
	50 and above	11	10.7
Education	HND/B.Sc	31	30.1
	M.Sc/MBA	52	50.5
	Ph.D	9	8.7
	Professional certification only	11	10.7
Organisational role	Information-security officer (ISM/CISO)	17	16.5
	Fraud-risk manager	21	20.4
	Digital-forensic analyst	15	14.6
	Internal/IT auditor	24	23.3
	Compliance/risk officer	18	17.5
	IT manager	8	7.8
Experience	Below 5 years	22	21.4
	5 to 10 years	45	43.7
	11 to 15 years	24	23.3
	Above 15 years	12	11.7
Total		103	100.0

Source: Field Survey, 2026.

Descriptive Statistics

Table 3 reports the construct means and dispersions. Judged against a midpoint of 3.0 on the five-point scale, all three competence dimensions drew broad agreement, with personnel expertise rated highest ($M = 3.88$, $SD = 0.69$), evidence analysis capability close behind ($M = 3.81$, $SD = 0.71$), and tools sophistication a little lower ($M = 3.68$, $SD = 0.74$). Cybersecurity

culture recorded the lowest mean of the five constructs ($M = 3.52$, $SD = 0.77$), an early indication that respondents view their security culture as only moderately mature and a foreshadowing of the constraint the moderation test probes. Detection effectiveness itself stood at $M = 3.79$ ($SD = 0.67$), a respectable but improvable level that squares with the mixed loss record set out earlier.

Table 3: Descriptive Statistics

Variable	N	Min	Mean	Std Dev
Digital Evidence Analysis Capability (DEAC)	103	2.00	3.81	0.71
Digital Forensic Tools Sophistication (DFTS)	103	1.80	3.68	0.74
Digital Forensic Personnel Expertise (DFPE)	103	2.00	3.88	0.69
Cybersecurity Culture (CSC)	103	1.60	3.52	0.77
Cyber-Fraud Detection Effectiveness (CFDE)	103	1.75	3.79	0.67

Source: SmartPLS output, Field Survey, 2026. N = 103 for all variables.

Measurement Model Assessment

The measurement model was examined for indicator reliability, internal consistency, and convergent validity, with results in Table 4 and the estimated model in Figure 2. Every outer loading fell between 0.771 and 0.861, clearing the 0.70 mark and confirming indicator reliability. Cronbach's Alpha (0.811 to 0.879), rho_A (0.818 to 0.884), and composite reliability (0.876 to

0.911) all exceeded 0.70, so internal consistency held across the five constructs. Convergent validity was equally secure: each average variance extracted (AVE) value, from 0.639 to 0.714, surpassed the 0.50 benchmark, meaning that every construct accounted for more than half the variance in its indicators (Hair et al., 2022). The constructs were therefore fit for structural estimation.

Table 4: Construct Reliability and Convergent Validity

Construct	Items	Loadings	α	ρ_A	CR	AVE
DEAC	4	0.781 - 0.852	0.842	0.851	0.894	0.679
DFTS	4	0.771 - 0.838	0.811	0.818	0.876	0.639
DFPE	4	0.802 - 0.861	0.866	0.872	0.909	0.714
CSC	4	0.778 - 0.844	0.828	0.835	0.886	0.661
CFDE	5	0.784 - 0.851	0.879	0.884	0.911	0.672

Source: SmartPLS output, 2026. Thresholds: loadings > 0.70; α , ρ_A , CR > 0.70; AVE > 0.50.

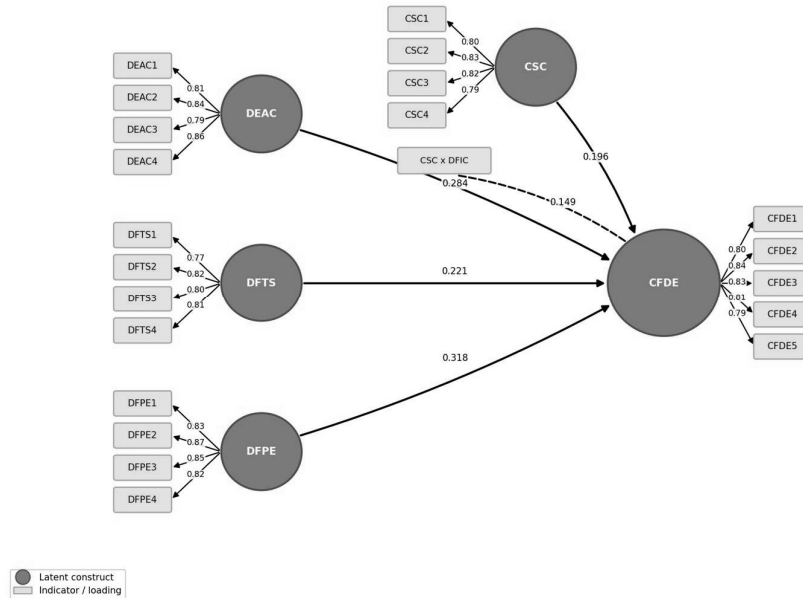


Figure 2: Measurement and Structural Model

Discriminant Validity

Discriminant validity was tested two ways. Under the Fornell and Larcker criterion (Table 5), the square root of each construct's AVE, shown on the bold diagonal, exceeded that construct's correlations with every other, so the constructs are distinct. The HTMT ratios (Table 6) tell the same story, each falling

beneath the conservative 0.85 ceiling (Henseler et al., 2015; Hair et al., 2022). That the five constructs correlate positively yet remain separable is theoretically sensible: firms with mature analysis, capable tools, expert staff, and a strong culture also tend to detect more fraud, but none of these is a proxy for another.

Table 5: Discriminant Validity (Fornell and Larcker Criterion)

	DEAC	DFTS	DFPE	CSC	CFDE
DEAC	0.824				
DFTS	0.541	0.799			
DFPE	0.557	0.529	0.845		
CSC	0.512	0.498	0.534	0.813	
CFDE	0.598	0.566	0.627	0.561	0.820

Diagonal (bold) = square root of AVE; off-diagonal = construct correlations.

Table 6: Discriminant Validity (HTMT Ratio)

	DEAC	DFTS	DFPE	CSC
DFTS	0.641			
DFPE	0.648	0.627		
CSC	0.611	0.602	0.629	
CFDE	0.697	0.672	0.718	0.651

All HTMT values fall below the 0.85 threshold.

Structural Model and Hypothesis Testing

With the measurement model secure, attention turned to structural estimation, summarised in Table 7. The model accounted for 61.2% of the variance in detection effectiveness ($R^2 = 0.612$;

adjusted $R^2 = 0.589$), a substantial figure for behavioural research, and the Stone-Geisser Q^2 of 0.398 confirmed predictive relevance. Effect sizes ranged from small to medium, with personnel expertise contributing the largest individual f^2 , a pattern that anticipates the path results.

Table 7: Structural Model Quality Criteria

Criterion	Value	Interpretation
R^2 (CFDE)	0.612	Substantial explanatory power
Adjusted R^2	0.589	Robust after adjusting for predictors
Q^2 (CFDE)	0.398	Predictive relevance established (> 0)
f^2 - DEAC	0.118	Small to medium effect
f^2 - DFTS	0.079	Small effect
f^2 - DFPE	0.142	Medium effect
f^2 - CSC (direct)	0.068	Small effect
f^2 - DFIC $\times$ CSC	0.049	Small but significant moderation

Source: SmartPLS output, 2026.

Path significance was established by bootstrapping 5,000 subsamples; Table 8

reports the coefficients and Figure 3 depicts the t-statistics.

Table 8: Path Coefficients and Hypothesis Testing (5,000 bootstrap subsamples)

Path	β	SE	t-value	p-value	Decision
DEAC $\rightarrow$ CFDE	0.284	0.078	3.642	0.000	Ho1 rejected
DFTS $\rightarrow$ CFDE	0.221	0.074	2.987	0.003	Ho2 rejected
DFPE $\rightarrow$ CFDE	0.318	0.077	4.115	0.000	Ho3 rejected
CSC $\rightarrow$ CFDE (direct)	0.196	0.077	2.534	0.011	Significant
DFIC $\times$ CSC $\rightarrow$ CFDE	0.149	0.062	2.413	0.016	Ho4 rejected

Source: SmartPLS output, 2026. β = standardised path coefficient.

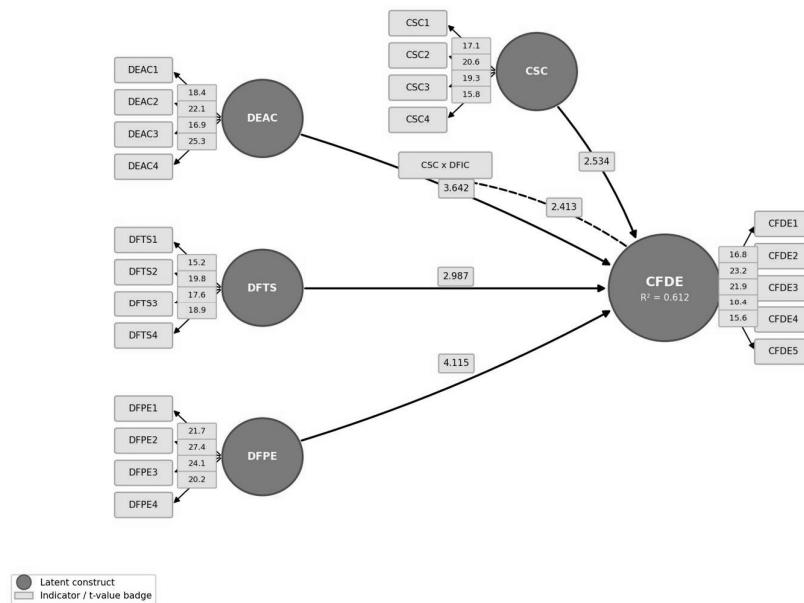


Figure 3: Structural Model, Bootstrapping (t-statistics)

Discussion of Findings

The first hypothesis held that evidence analysis capability has no effect on detection. It did not survive the data ($\beta = 0.284$, $t = 3.642$, $p = 0.000$), so Ho1 is rejected. The reading is straightforward: the more disciplined a firm is in acquiring, preserving, and interrogating digital traces, the more of its fraud it catches, because it is careful handling that turns raw logs into the signal detection depends on. The result echoes Awodiran et al. (2023) on the detection gains from forensic accounting techniques in Nigerian financial entities and Dubey et al. (2023) on the reliability that advanced analysis brings. Framed by the resource-based view (Barney, 1991; Wernerfelt, 1984), analytical capability behaves as a valuable, firm-specific resource that feeds directly into performance.

The second hypothesis fared no better ($\beta = 0.221$, $t = 2.987$, $p = 0.003$); Ho2 is rejected. Breadth, currency, and integration in the toolset improve detection by exposing anomalies that manual review lets slip, a finding in line with Dubey et al. (2023) and Aziz and Andriansyah (2023) on the value of sophisticated and AI-driven analytics, and with Akinbowale et al. (2023) on advanced techniques in fraud-risk mitigation. That tooling carries the smallest of the three direct coefficients is itself informative: instruments deliver much of their value through the analysts who operate them, so their independent contribution, while real, is partly mediated by expertise.

Personnel expertise produced the strongest effect in the model ($\beta = 0.318$, $t = 4.115$, $p = 0.000$), and Ho3 is rejected.

Detection, in the end, is exercised by people, and the certification, experience, and judgement of investigators set the ceiling on how accurately and defensibly a firm can act. The result supports Afriyie et al. (2023) on the decisiveness of forensic competence and Micah et al. (2023) on the skill demands facing Nigerian practitioners, and it accords with Daraojimba et al. (2024), who place investigator competence at the centre of digital financial fraud prevention. The primacy of expertise over tooling is one of the study's more pointed messages for firms tempted to solve detection by procurement alone.

The fourth hypothesis addressed the study's central claim. The interaction term was positive and significant ($\beta = 0.149$, $t = 2.413$, $p = 0.016$), so H_4 is rejected, and cybersecurity culture also acted directly on detection ($\beta = 0.196$, $t = 2.534$, $p = 0.011$). As culture strengthens, the competence-to-detection relationship steepens, because firms with a healthy culture escalate anomalies, protect evidence, and convert investigative output into action rather than letting it lapse. The finding is consistent with Da Veiga et al. (2020) and Uchendu et al. (2021) on the weight of security culture, and it makes sense of the uneven returns to forensic investment reported by Akinbowale et al. (2021) and Olaiya et al. (2024) by naming the conditioning factor explicitly. In resource-based terms (Barney, 1991), culture is the organising capability that turns forensic resources into advantage, and the technology-organisation-environment framework (Tornatzky & Fleischer, 1990) accounts for why the same

resources are detected unevenly across organisational contexts.

Conclusion and Recommendations

This study set out to establish whether cybersecurity culture governs the detection returns to forensic investigation competence among Nigerian fintechs, and the evidence answers in the affirmative on every count. Personnel expertise was the strongest driver of detection, confirming that a forensic function realises its value chiefly through the proficiency of its investigators. Evidence analysis capability and tools sophistication each raised detection independently, establishing careful evidence handling and capable tooling as measurable antecedents rather than incidental features. Cybersecurity culture mattered twice over, lifting detection directly and, more tellingly, amplifying the payoff to competence. The larger lesson is that the detection dividend in Nigeria's fintech sector depends not only on how well firms analyse evidence, equip investigators, and staff the forensic function, but on whether the surrounding culture allows that capability to work.

Several recommendations follow from the evidence:

- i. Fintech boards should treat the development of forensic personnel as a first-order investment, funding certifiable training and recruiting experienced investigators, since personnel expertise carried the strongest effect on detection.
- ii. Management should cultivate cybersecurity culture deliberately, through visible leadership commitment, open incident reporting,

- and consistency between stated policy and daily practice, because culture both raised detection directly and magnified the returns to competence.
- iii. Firms should renew and integrate their forensic tooling towards automated, analytics-driven, and machine-learning-enabled platforms interoperable with transaction monitoring, so that capable instruments continue to surface the anomaly detection relies on.
 - iv. Firms should embed rigorous acquisition, preservation, and analysis procedures with documented chain of custody, given the confirmed contribution of evidence analysis capability.
 - v. The Central Bank of Nigeria, the FinTech Association of Nigeria, and allied supervisors should build forensic-capability and security-culture benchmarks into supervisory expectations and industry standards, backed by capacity-building, in light of the rising national fraud-loss environment.
- The study's limits qualify these claims in the usual ways. A cross-sectional design fixes the relationships at one moment and cannot settle causality, which longitudinal work would help resolve. Self-reported perceptions of detection invite social-desirability bias, tempered here by anonymity. The focus on nationally supervised fintechs sharpens analytical depth but narrows generalisation to unregulated operators and to other African markets. Future research could carry the model into several jurisdictions, adopt longitudinal or mixed methods designs, and test further moderators such as regulatory intensity, board oversight, or threat exposure.

References

- Afriyie, S. O., Akomeah, M. O., Amoakohene, G., Ampimah, B. C., Ocloo, C. E., & Kyei, M. O. (2023). Forensic accounting: A novel paradigm and relevant knowledge in fraud detection and prevention. *International Journal of Public Administration*, 46(9), 615–624.
<https://doi.org/10.1080/01900692.2021.2009855>
- Akinbowale, O. E., Klingelhofer, H. E., & Zerihun, M. F. (2020). An innovative approach in combating economic crime using forensic accounting techniques. *Journal of Financial Crime*, 27(4), 1253–1271.
- <https://doi.org/10.1108/JFC-04-2020-0053>
- Akinbowale, O. E., Klingelhofer, H. E., & Zerihun, M. F. (2021). The integration of forensic accounting and the management control system as tools for combating cyberfraud. *Academy of Accounting and Financial Studies Journal*, 25(2), 1–14.
- Akinbowale, O. E., Klingelhofer, H. E., & Zerihun, M. F. (2023). Application of forensic accounting techniques in the South African banking industry for the purpose of fraud risk mitigation. *Cogent Economics & Finance*, 11(1), 1–21.

- <https://doi.org/10.1080/23322039.2022.2153412>
- Awodiran, M. A., Ogundele, A. T., Idem, U. J., & Emem, O. (2023). Digital forensic accounting and cyber fraud in Nigeria. In *2023 International Conference on Cyber Management and Engineering (CyMaEn)* (pp. 321–326). IEEE. <https://doi.org/10.1109/CyMaEn57228.2023.10050992>
- Aziz, L. A. R., & Andriansyah, Y. (2023). The role of artificial intelligence in modern banking: An exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. *Reviews of Contemporary Business Analytics*, 6(1), 110–132.
- Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, 17(1), 99–120. <https://doi.org/10.1177/014920639101700108>
- Bharadwaj, A. S. (2000). A resource-based perspective on information technology capability and firm performance: An empirical investigation. *MIS Quarterly*, 24(1), 169–196. <https://doi.org/10.2307/3250983>
- Central Bank of Nigeria. (2024). *Financial stability report*. Central Bank of Nigeria.
- Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture: Perspectives from academia and industry. *Computers & Security*, 92, 101713. <https://doi.org/10.1016/j.cose.2020.101713>
- Daraojimba, R. E., Farayola, O. A., Olatoye, F. O., Mhlongo, N., & Oke, T. T. (2024). Forensic accounting in the digital age: A U.S. perspective: Scrutinizing methods and challenges in digital financial fraud prevention. *Finance & Accounting Research Journal*, 6(2), 241–260.
- Dubey, H., Bhatt, S., & Negi, L. (2023). Digital forensics techniques and trends: A review. *The International Arab Journal of Information Technology*, 20(4), 644–654.
- Federal Republic of Nigeria. (2024). *Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024*. Federal Government Printer.
- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39–50. <https://doi.org/10.1177/002224378101800104>
- Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). *A primer on partial least squares structural equation modeling (PLS-SEM)* (3rd ed.). Sage Publications.
- Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, 31(1), 2–24. <https://doi.org/10.1108/EBR-11-2018-0203>
- Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43(1), 115–135.

- <https://doi.org/10.1007/s11747-014-0403-8>
- Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of e-Collaboration*, 11(4), 1–10. <https://doi.org/10.4018/ijec.2015100101>
- Micah, E. E. M., Saidu, I. H., Ibitomi, T., & Sanusi, B. S. (2023). Digital forensics in the era of cybercrime: Emerging trends and challenges for forensic accountants in Nigeria. *European Journal of Accounting, Auditing and Finance Research*, 11(9), 85–100.
- Nigeria Inter-Bank Settlement System. (2025). *Annual fraud report 2024*. NIBSS.
- Ogwiji, J., & Lasisi, I. O. (2022). Internal control system and fraud prevention of quoted financial services firms in Nigeria: A SmartPLS-SEM approach. *European Journal of Accounting, Auditing and Finance Research*, 10(4), 1–33.
- Olaiya, O. P., Adesoga, T. O., Ojo, A., Olagunju, O. D., Ajayi, O. O., & Adebayo, Y. O. (2024). Cybersecurity strategies in fintech: Safeguarding financial data and assets. *GSC Advanced Research and Reviews*, 20(1), 50–56. <https://doi.org/10.30574/gscarr.2024.20.1.0241>
- Sarstedt, M., Ringle, C. M., & Hair, J. F. (2022). Partial least squares structural equation modeling. In C. Homburg, M. Klarmann, & A. Vomberg (Eds.), *Handbook of market research* (pp. 587–632). Springer. https://doi.org/10.1007/978-3-319-57413-4_15
- Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington Books.
- Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, 109, 102387. <https://doi.org/10.1016/j.cose.2021.102387>
- Wernerfelt, B. (1984). A resource-based view of the firm. *Strategic Management Journal*, 5(2), 171–180. <https://doi.org/10.1002/smj.4250050207>