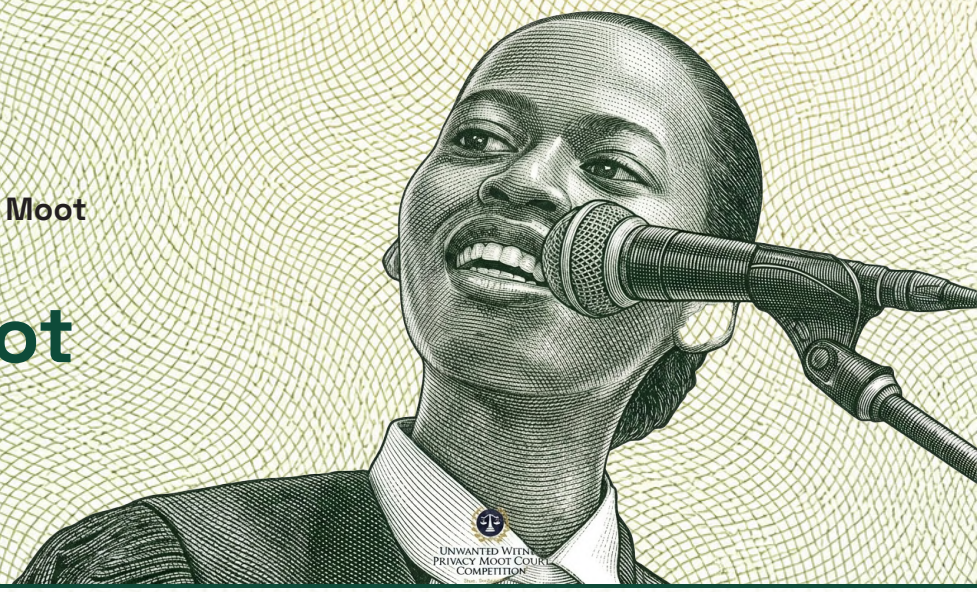
UNWANTED WITNESS PRIVACY MOOT COURT COMPETITION

Dare . Participate . Win

5 ANNIVERSARY



Unwanted Witness Privacy Moot Court Competition 2026

# Official Moot Problem

## THE EAST AFRICAN DIGITAL RIGHTS COURT

(A Fictional Regional Human Rights Court)

**Amani Kato & 3 Others**
**v.**
**FinCredit Technologies Ltd, Telelink Communications Plc, and the Republic of Kisiwa**

Unwanted Witness Privacy Moot Court Competition 2026
Official Moot Problem

**Theme:**
Protecting Personal Data in Digital Financial Services and Fintech Ecosystems in East Africa

UNWANTED WITNESS

"Amplifying Voices, Changing lives"

www.unwantedwitness.org

## I. STATEMENT OF FACTS

### A. The Regional Context

1. *The East African Community (EAC)* is a regional economic bloc composed (for the purposes of this moot problem), of four fictional member states: the *Republic of Kisiwa*, *the Republic of Nembia*, *the United Republic of Tavola*, and *the Republic of Buranda*.

2. The member states of the *EAC* have adopted several regional initiatives aimed at promoting economic integration and digital trade within the region. These initiatives include regional digital commerce agreements, cross-border financial interoperability frameworks, and policy coordination mechanisms for the regulation of financial technology (fintech) services.

3. As part of these efforts, the *EAC* has encouraged the development of interoperable digital payment systems allowing mobile money providers and financial institutions in different member states to process electronic payments and remittances across borders.

4. Over the past decade, the region has experienced rapid growth in digital financial services driven by widespread mobile phone penetration, expanding internet connectivity, and increasing demand for alternative sources of credit.

5. Financial services in the region have increasingly shifted from traditional banking channels to mobile-based financial platforms, including mobile money services, app-based lending platforms, digital banking applications, and cross-border electronic payment services.

6. These services have played a significant role in expanding financial inclusion, particularly among individuals and small businesses that previously lacked access to conventional banking services.

7. By 2025, more than seventy percent (70%) of adults within the region were estimated to be active users of mobile financial services, with millions relying on mobile money platforms for daily transactions such as payments, remittances, savings, and short-term borrowing.

8. At the same time, the rapid expansion of digital financial services has led to the emergence of a growing fintech sector in which technology companies provide financial services through digital platforms rather than traditional banking infrastructure.

9. One of the most rapidly expanding segments of this sector has been digital lending, in which mobile applications allow users to obtain short-term loans through automated approval systems.

10. While digital lending services have been widely promoted as a tool for financial inclusion and economic empowerment, their operation has also raised regulatory concerns regarding consumer protection, data privacy, and the collection and processing of personal data within digital financial ecosystems.

### B. Digital Lending and Data-Driven Credit Scoring

11. In recent years, the expansion of mobile phone usage and mobile money services across the *East African Community* has led to the rapid growth of digital lending platforms. These platforms provide short-term loans through smartphone applications, allowing users to obtain credit without visiting traditional financial institutions.

12. Unlike conventional banking systems, which typically rely on collateral, income verification, and formal credit histories, digital lending platforms in the region frequently rely on *data-driven credit scoring models*. These models use automated systems to evaluate an individual's creditworthiness based on patterns derived from digital activity.

13. To generate such credit assessments, digital lenders collect and analyze large volumes of behavioral and transactional data obtained from users' smartphones and associated financial services. The categories of data commonly collected include *mobile money transaction records*, *call logs* and *SMS metadata*, *geolocation history*, *lists of installed applications*, *device identifiers linked to individual users*, and *contact lists* stored on the user's mobile device.

*14.* *Fintech* companies assert that these forms of data provide insight into a borrower's financial behavior and reliability. By analyzing patterns such as transaction frequency, communication networks, and device usage, lenders claim to be able to estimate the likelihood that a borrower will repay a loan.

15. These data inputs are processed through automated credit scoring systems that use statistical models and machine-learning techniques to generate individualized credit profiles. The resulting scores are used to determine whether an applicant qualifies for a loan and, if so, under what conditions.

16. In practice, the credit score generated by these systems may influence several aspects of the lending decision, including whether a loan application is approved, the amount of credit extended to the borrower, the applicable interest rate, and the level of perceived repayment risk associated with the borrower.

17. Because these determinations are made through automated systems operating within digital platforms, loan approval or rejection decisions are frequently generated within seconds and without direct human review.

18. Supporters of these technologies argue that such systems expand financial inclusion by enabling individuals without formal credit histories to access credit. Critics, however, have raised concerns that the extensive collection and processing of personal and behavioral data may create risks for privacy, transparency, and accountability in digital financial ecosystems.

### C. The FlashCredit Platform

*19.* *FinCredit* Technologies Ltd is a financial technology company incorporated under the laws of the *Republic of Nembia*. The company provides digital lending services across several member states of the East African Community through a smartphone-based lending platform known as *FlashCredit.*

*20.* *FlashCredit* was launched in *2022* as part of *FinCredit*'s strategy to expand access to short-term microcredit for individuals who lack access to traditional banking services. The platform is marketed primarily to small traders, students, informal workers, and other individuals who may not possess formal credit histories.

21. The *FlashCredit* application enables users to apply for and receive small short-term loans directly through their mobile devices without the need for physical documentation or in-person verification.

22. Through the platform, users may request loans ranging from *USD 5 to USD 200*, with repayment periods typically ranging between *seven (7) and thirty (30) days.*

23. Loan applications submitted through *FlashCredit* are processed automatically by an algorithmic credit assessment system known as the *Financial Trust Score (FTS).*

24. The *FTS* is a proprietary automated scoring system developed by *FinCredit* in collaboration with third-party analytics providers. The system evaluates a combination of financial, behavioral, and device-related data associated with the applicant.

25. Based on this analysis, the system automatically determines:

    a. whether the applicant qualifies for a loan;
    b. the amount of credit to be offered;
    c. the interest rate applicable to the loan; and
    d. the repayment period assigned to the borrower.

28. The approval or rejection of loan applications occurs within seconds of submission and typically involves *no human review*.

*29.* *FinCredit* advertises the *FlashCredit* platform as*: "A fully automated credit system designed to expand financial inclusion by providing instant digital loans to underserved populations."*

30. According to *FinCredit's* public materials, the platform relies on *advanced data analytics and automated risk modelling* to assess borrower reliability in environments where traditional credit information may be unavailable.

31. By 2025, *FlashCredit* had reportedly been downloaded by more than *three million users across the East African region*, with a significant portion of its users residing in the *Republic of Kisiwa*.

### D. Partnerships within the Fintech Ecosystem

32. In order to operate its digital lending services across the region, *FinCredit Technologies Ltd* entered into a number of commercial partnerships with entities involved in telecommunications infrastructure, data analytics, and credit information sharing.

33. These partnerships formed part of *FinCredit's* broader strategy to integrate digital financial services with existing mobile communications and data-processing ecosystems within the *East African Community*.

#### 1. Telelink Communications Plc

34. Telelink Communications Plc is the largest telecommunications operator in the *Republic of Kisiwa* and the provider of the mobile money platform *T-Money*, which accounts for approximately *sixty-five percent* of all digital financial transactions conducted within the country.

35. As part of a commercial integration agreement concluded in *2023, Telelink* granted *FinCredit* access to certain categories of data associated with users of the *T-Money* platform.

36. Under the terms of the agreement, *FinCredit* was permitted to obtain transaction-related metadata generated through the use of *T-Money* accounts, including records relating to payment transfers, account activity, and transaction frequency.

37. The agreement also enabled *FinCredit* to access subscriber registration information associated with *T-Money* accounts, including mobile subscriber identity details and device identifiers linked to the user's mobile handset.

*38.* *Telelink* maintained that the data shared with *FinCredit* was necessary to facilitate automated credit assessments and fraud-prevention mechanisms within the *FlashCredit* platform.

**2. DataMind Analytics Ltd**

39. *FinCredit* also entered into a contractual arrangement with *DataMind Analytics Ltd*, a data analytics and machine-learning firm incorporated in the *United Republic of Tavola*.

40. *DataMind* was responsible for designing and maintaining the algorithmic models used by *FinCredit* to generate the *Financial Trust Score (FTS)* employed in the *FlashCredit* lending system.

41. The models developed by *DataMind* relied on the analysis of large datasets derived from borrower transaction records, device metadata, and behavioral indicators associated with mobile phone usage.

42. Data processing for these analytical functions was conducted through cloud-based infrastructure operated by *DataMind* and hosted in several jurisdictions outside the *East African Community*.

43. The precise location of the cloud servers and the legal framework governing such cross-border data processing were not publicly disclosed by either *FinCredit* or *DataMind*.

**3. Regional Credit Reference Bureau**

44. *FinCredit* also participated in a regional credit information exchange platform administered by the *Regional Credit Reference Bureau (RCRB)*.

45. The *RCRB* operates a centralized system through which participating lenders may submit and access credit histories relating to borrowers within participating states.

46. Through its participation in the platform, *FinCredit* was able to submit information regarding borrower repayment behavior and to obtain credit histories maintained by other financial institutions operating within the region.

47. The information exchanged through the *RCRB* platform was used by *FinCredit* as an additional factor in the calculation of its automated credit scoring system.

**E. Installation and Data Permissions**

48. Individuals wishing to obtain loans through the *FlashCredit* platform must first download and install the *FlashCredit* mobile application from a digital application marketplace.

49. Upon launching the application for the first time, users are required to create a personal account linked to their mobile phone number and mobile money wallet.

50. During the installation and account registration process, the application displays a series of permission requests seeking access to data stored on the user's device.

51. These permission requests appear through standard operating system prompts requiring the user to select either *"Allow"* or *"Deny"* in order to proceed.

52. The permissions requested by the *FlashCredit* application include *access to the user's contact list*, *call logs*, *SMS metadata*, *geolocation data*, *installed applications*, *device identifiers*, and *mobile money transaction history* associated with the device.

53. The application informs users that these permissions are necessary for the operation of the *FlashCredit* service, including identity verification, fraud detection, and automated credit scoring.

54. Users who decline any of the requested permissions are unable to complete the account registration process and cannot access the lending services offered by the application.

55. During the installation process, users are also required to accept the *FlashCredit* Privacy and Data Use Agreement.

56. The Privacy and Data Use Agreement is accessible through a hyperlink embedded in the application interface.

57. The policy consists of approximately *thirty-two (32) pages* of legal text describing the categories of personal data collected by the platform, the purposes of processing such data, and the circumstances under which the data may be shared with third-party service providers.

58. The policy is available only in English and is presented in a scrollable text format within the application interface.

59. The application requires users to indicate acceptance of the Privacy and Data Use Agreement by selecting an *"I Agree"* button before accessing the FlashCredit services.

60. The policy also states that certain categories of user data may be processed through cloud-based infrastructure located in jurisdictions outside the *East African Community*.

## F. Events Concerning the Individual Applicants

61. The Applicants are individuals residing in the *Republic of Kisiwa* who at various times interacted with the *Flash-Credit* digital lending platform.

### 1. Amani Kato

62. In *March 2024*, *Amani Kato*, a small retail trader operating a kiosk in the city of *Luranda*, downloaded the *Flash-Credit* mobile application from the *T-Market mobile* application store.

63. During installation of the application, the platform requested permission to access several categories of data from Amani's mobile device, including *contact lists*, *SMS metadata*, *device identifiers*, and *mobile money transaction history* associated with his *T-Money* account.

64. After accepting the requested permissions, *Amani* applied for a short-term digital loan through the application. Within seconds, the *FlashCredit* platform approved a loan of *USD 50*, which was disbursed through the *T-Money* mobile wallet linked to his *phone number*.

65. The approval decision was generated automatically by the *FlashCredit* algorithmic credit-scoring system known as the *Financial Trust Score (FTS)*.

66. In *April 2024*, *Amani* experienced a decline in business revenues following supply shortages affecting several local markets. As a result, he failed to repay the loan within the repayment period specified in the application.

67. Shortly thereafter, several individuals listed in *Amani's mobile phone contact list* informed him that they had received automated text messages referencing his loan.
68. According to screenshots later shared with *Amani*, the message read: "*Your contact AMANI KATO has an outstanding loan with FlashCredit. Kindly remind them to repay immediately.*"

*69.* *Amani* states that he did not authorize the disclosure of information concerning his loan status to any third party.

*70.* *FinCredit* maintains that such messages are generated automatically through its recovery notification system and are intended to encourage repayment.

### 2. Grace Namugenyi

71. In *May 2024*, *Grace Namugenyi*, a second-year law student at the *University of Kisiwa*, downloaded the *FlashCredit* application after learning about the platform through social media advertisements promoting "*instant credit for students.*"

72. After completing the registration process, *Grace* submitted an application for a digital loan of *USD 30* through the application interface.

73. The application was rejected within seconds.

74. The application interface displayed a notification stating that the request had been declined because *Grace's* Financial Trust Score did not meet the minimum lending threshold.

*75.* *Grace* subsequently submitted a request through the *FlashCredit in-app* customer support function asking for clarification regarding the basis on which her application had been rejected.

76. A customer support representative responded that lending decisions were generated automatically by the platform's scoring algorithm and that additional details regarding the scoring methodology could not be disclosed.

*77.* *Grace* maintains that the explanation provided did not clarify what data had been used in calculating her score or whether the data relied upon was accurate.

### 3. David Mwangi

*78.* *David Mwangi*, a motorcycle taxi driver operating in the *capital city of Kisiwa*, had used the *FlashCredit* platform several times between *2023* and early *2024*.

79. During this period, *David* obtained and repaid several short-term digital loans through the application.

80. Following public discussion surrounding *Grace Namugenyi's* complaint regarding algorithmic lending decisions, David sought to review the personal data associated with his account.

*81.* *David* accessed the *FlashCredit* application interface and searched for options that would allow him to view or download the personal data stored about him by the platform.

82. According to *David,* the application interface did not provide any function allowing users to *access, correct*, or *delete*

the personal data associated with their accounts.

83. David subsequently sent an email inquiry to the *FlashCredit* customer support address requesting information regarding the data held about him.

84. At the time the present proceedings were initiated, David had not received any substantive response to this request.

### G. The Data Security Incident

85. In *June 2024*, a group of independent cybersecurity researchers affiliated with the *Digital Security Observatory* published a report indicating that a database connected to the *FlashCredit* lending platform had been exposed on a publicly accessible cloud server.

86. According to the report, the database was hosted on a cloud infrastructure service used by *DataMind Analytics Ltd*, a third-party data analytics contractor engaged by *FinCredit* to process borrower data for credit scoring purposes.

87. The researchers stated that the server had been misconfigured in a manner that allowed external access without authentication through an unsecured *Application Programming Interface (API)*.

88. The exposed dataset reportedly contained records relating to more than *500,000 FlashCredit borrowers* across several East African states.

89. The dataset included, inter alia:

- borrower phone numbers
- national identification numbers
- loan histories
- repayment records
- mobile money transaction summaries
- device identifiers associated with borrower accounts.

1. The researchers indicated that the exposed database appeared to have been publicly accessible for an undetermined period prior to its discovery.

2. The report further noted that the data structure suggested integration between *FlashCredit* user accounts and mobile money transaction records obtained from the *T-Money* platform operated by *Telelink Communications Plc.*

3. Following publication of the report, several technology news outlets reported on the alleged data exposure and raised concerns regarding the security practices of digital lending platforms operating in the region.

4. In response to the report, *FinCredit* issued a public statement indicating that the exposed database belonged to a *third-party analytics contractor* and that no financial accounts or payment systems had been compromised.

5. *FinCredit* further stated that the data exposure did not affect the operational integrity of the *FlashCredit* platform and that remedial measures had been taken to secure the affected server.

6. However, the statement did not specify the duration of the exposure, the exact categories of data involved, or whether affected borrowers had been individually notified of the incident.

7. The cybersecurity researchers subsequently recommended that individuals whose data may have been included in the exposed dataset take precautionary measures due to the potential risk of identity theft or unauthorized profiling.

8. It remains disputed whether FinCredit had previously been alerted to vulnerabilities in the *DataMind analytics* infrastructure prior to the publication of the researchers' report.

## II. REGULATORY PROCEEDINGS

### A. Complaint to the Data Protection Authority

9. In *August 2024*, the Applicants jointly submitted a formal complaint to the *Kisiwa Data Protection Authority (KDPA)*, the statutory body responsible for enforcing data protection and privacy legislation in the Republic of Kisiwa.

10. The complaint alleged that the data practices of *FinCredit Technologies Ltd and Telelink Communications Plc* violated several principles of data protection law, including the principles of *lawful processing*, *data minimization*, *purpose limitation*, and *data security*.

11. In particular, the Applicants alleged that the *FlashCredit* application collected extensive categories of personal data from users' mobile devices that were not necessary for the provision of digital lending services.

12. The Applicants further alleged that the application processed personal data without obtaining *free, specific, informed,* and *unambiguous consent*, noting that access to the lending service was conditional upon acceptance of a lengthy privacy policy presented through the mobile application interface.

13. The complaint also asserted that *FinCredit* had shared personal data with third-party entities, including *DataMind Analytics Ltd* and the *Regional Credit Reference Bureau*, without providing adequate notice to users or obtaining explicit authorization for such disclosures.

14. The Applicants further alleged that *Telelink Communications Plc* had unlawfully transmitted *mobile money transaction data* and *subscriber information* associated with *T-Money accounts* to *FinCredit* pursuant to a commercial data-sharing arrangement.

15. According to the Applicants, such data sharing occurred without the knowledge of the affected subscribers and exceeded the purposes for which the data had originally been collected by *Telelink*.

16. The complaint additionally raised concerns regarding the data security incident reported in *June 2024*, arguing that the exposure of borrower records demonstrated a failure by FinCredit to implement appropriate technical and organizational safeguards to protect personal data against unauthorized access.

17. The Applicants requested that the *KDPA* investigate the data processing activities of *FinCredit* and *Telelink* and determine whether the practices complied with applicable data protection and privacy regulations.

### B. Decision of the KDPA

18. On *15 January 2025*, the *Kisiwa Data Protection Authority (KDPA)* issued its decision in response to the complaint filed by the Applicants concerning the data practices of *FinCredit Technologies Ltd* and *Telelink Communications Plc*.

19. In its decision, the *Authority* noted that the *FlashCredit* application required users to accept the *FlashCredit Privacy and Data Use Agreement* at the time of installation in order to access the lending service.

20. The *Authority* observed that the privacy policy disclosed that certain categories of personal data, including *mobile device identifiers*, *transaction metadata*, and *contact information*, could be collected and processed for the purposes of credit scoring, fraud prevention, and risk management.

21. The *Authority* further stated that digital lending platforms operating within the region commonly relied on automated data analytics and behavioral data to generate creditworthiness assessments for prospective borrowers.

22. According to the *Authority*, such practices appeared to reflect prevailing industry standards in digital financial services and were considered integral to the operation of automated lending platforms.

23. With regard to the allegations concerning the sharing of mobile money transaction data between *Telelink Communications Plc* and *FinCredit Technologies Ltd*, the *Authority* noted that the parties had entered into a commercial data-sharing arrangement connected to the operation of the *FlashCredit* platform.

24. The *Authority* stated that the available documentation suggested that the data shared under this arrangement was intended to support credit risk analysis and algorithmic scoring models used by the *FlashCredit* system.

25. The *Authority* also considered the *Applicants*' allegations concerning cross-border processing of borrower data through cloud infrastructure operated by *DataMind Analytics Ltd*.

26. In this regard, the *Authority* observed that certain data processing activities connected to the *FlashCredit* platform appeared to take place on servers located outside the territory of the *Republic of Kisiwa*.

27. The *Authority* concluded that, insofar as those processing activities occurred in jurisdictions beyond the territorial scope of its regulatory mandate, they did not fall within the direct enforcement jurisdiction of the *KDPA*.

28. In light of these considerations, the *Authority* determined that the available information did not establish a violation of the applicable data protection obligations under the laws of the *Republic of Kisiwa*.

29. The complaint was therefore dismissed.

## III. NATIONAL COURT PROCEEDINGS

30. Following the decision of the *Kisiwa Data Protection Authority* in *January 2025*, the Applicants filed a constitutional petition before the *High Court of the Republic of Kisiwa*.

31. In their petition, the Applicants challenged the legality of the data practices undertaken by *FinCredit Technologies Ltd* and *Telelink Communications Plc*.

32. The Applicants argued that the collection, analysis, and disclosure of personal data through the *FlashCredit* platform violated their constitutional right to privacy and protection of personal information.

33. In particular, the Applicants alleged that:
    *a) FinCredit* had collected excessive personal data unrelated to the provision of digital credit services;
    *b) Telelink* had unlawfully shared subscriber transaction data with *FinCredit* without lawful authorization;
    c) the automated credit scoring system used by *FlashCredit* constituted opaque profiling that affected individuals without transparency or meaningful oversight.

34. The *Respondents* opposed the petition and argued that the Applicants had voluntarily consented to the processing of their personal data when installing and using the *FlashCredit* application.
35. *FinCredit* further argued that the collection and analysis of behavioral and transactional data formed a necessary component of digital lending models, particularly those designed to provide financial services to individuals lacking traditional credit histories.

36. *Telelink Communications Plc* submitted that the transaction data shared with *FinCredit* had been processed in accordance with commercial agreements and industry practices within the digital financial services sector.

37. On *22 May 2025*, the *High Court of Kisiwa* delivered judgment dismissing the Applicants' petition.

38. The Court held that individuals who voluntarily install and use digital financial service applications must be understood to have accepted the data processing practices associated with such platforms.

39. The Court further observed that digital financial technologies rely heavily on data analytics and algorithmic decision-making, which it characterized as an essential feature of contemporary financial innovation.

40. The Court concluded that the *Applicants* had not demonstrated that the *Respondents*' conduct constituted an unlawful interference with the constitutional right to privacy.

41. Dissatisfied with the decision, the Applicants filed an appeal before the *Supreme Court of the Republic of Kisiwa*.

42. In their appeal, the Applicants argued that the *High Court* had failed to adequately consider the implications of automated profiling, cross-border data transfers, and the lack of meaningful consent mechanisms within the *FlashCredit* platform.

43. The Respondents maintained that the *High Court* had correctly interpreted the relationship between digital financial innovation and personal data practices.

44. In *October 2025*, the *Supreme Court* delivered its judgment dismissing the appeal.

45. The *Supreme Court* affirmed the reasoning of the *High Court* and emphasized the significant role played by digital financial services in advancing financial inclusion across the region.

46. The *Court* held that regulatory oversight of digital financial services should primarily fall within the competence of specialized regulatory authorities rather than the judiciary.

47. The *Supreme Court* therefore upheld the decision of the *High Court* and confirmed the dismissal of the Applicants' claims.

## IV. PROCEEDINGS BEFORE THE EAST AFRICAN DIGITAL RIGHTS COURT

48. On *14 February 2026*, the Applicants filed an application before the *East African Digital Rights Court* alleging that the conduct described in this case constituted violations of regional human rights obligations relating to the right to privacy and the protection of personal data.

49. The application was lodged pursuant to the jurisdiction of the Court under the regional human rights framework governing the member states of the *East African Community*. The Applicants contend that the acts and omissions of the Respondents engage the international responsibility of the *Republic of Kisiwa* for failing to ensure adequate protection of personal data within its jurisdiction.

50. The *Applicants* further argue that the actions of *FinCredit Technologies Ltd* and *Telelink Communications Plc* were undertaken with the knowledge or acquiescence of state authorities and within a regulatory environment overseen by the *Government of Kisiwa*.

51. Following the filing of the application, the *Respondents* submitted preliminary objections challenging the admissibility of the case.

52. The *Respondents* contend, inter alia, that the *Applicants* have failed to exhaust available domestic remedies, arguing that certain administrative remedies remained available under national data protection legislation at the time the application was filed.

53. The *Respondents* further submit that *FinCredit Technologies Ltd* and *Telelink Communications Plc* are private corporate entities and therefore cannot be held directly responsible under regional human rights law.

54. In addition, the *Respondents* argue that significant elements of the data processing activities described in the application occurred outside the territorial jurisdiction of the *Republic of Kisiwa* and beyond the regulatory authority of the *East African Digital Rights Court*.

55. The *Applicants* dispute these objections and maintain that domestic remedies were exhausted through proceedings before the *Kisiwa Data Protection Authority* and subsequent litigation before the *High Court* and *Supreme Court of Kisiwa.*

56. The *Applicants* also contend that the alleged violations arise from the failure of the *Republic of Kisiwa* to regulate digital financial services operating within its jurisdiction and to protect individuals from unlawful processing of personal data.

57. After considering the submissions of the parties, the *Court* determined that the questions relating to jurisdiction, admissibility, and the merits of the case were closely interconnected.

58. The Court therefore decided to join the preliminary objections to the merits of the case and to proceed with the hearing of the application.

## V. ANNEXES

The following documents form part of the record.

### ANNEX A: Excerpt from the *FlashCredit* Privacy and Data Use Agreement

*FlashCredit* Mobile Application
Privacy and Data Use Agreement

**Version 2.3**
Last Updated: 15 January 2024

This document constitutes an excerpt from the Privacy and Data Use Agreement governing the *FlashCredit* digital lending platform operated by *FinCredit Technologies Ltd.*

**1. Introduction**

1.1 *FlashCredit* is a digital lending platform operated by *FinCredit Technologies Ltd* that enables users to access short-term credit services through a mobile application.

1.2 The *FlashCredit* platform relies on automated data analytics and digital technologies to assess the creditworthiness of users and to deliver lending services through mobile devices.

1.3 This Privacy and Data Use Agreement describes how *FlashCredit* collects, processes, stores, and shares personal data in connection with the operation of its services.

1.4 By installing and using the *FlashCredit* application, users acknowledge that their personal data may be collected and processed in accordance with the provisions of this Agreement.

**2. Categories of Personal Data Collected**

2.1 *FlashCredit* may collect personal data directly from users during account registration and through the operation of the *FlashCredit* mobile application.

1.2 The categories of personal data collected may include:

a) mobile phone number associated with the user's account;
b) national identification number or other government-issued identification;
c) device identifiers associated with the user's mobile device;
d) geolocation information generated by the user's device;
e) records of mobile money transactions linked to the user's digital wallet;
f) contact lists stored on the user's mobile device;
g) call logs and SMS metadata generated by the device;
h) information concerning installed applications on the device.

2.3 *FlashCredit* may also generate derived data based on analysis of the information listed above, including behavioral indicators and creditworthiness profiles.

**3. Purposes of Data Processing**

3.1 Personal data collected through the *FlashCredit* platform may be processed for the following purposes:

a) verifying the identity of users;
b) preventing fraud and financial misconduct;
c) assessing creditworthiness through automated scoring systems;
d) determining loan eligibility, loan amount, and repayment terms;
e) monitoring loan repayment performance;
f) improving the functionality and security of the *FlashCredit* platform.

3.2 *FlashCredit* may also process personal data to conduct internal research and analytics aimed at improving financial risk modelling and product development.

**4. Automated Decision-Making**

4.1 *FlashCredit* utilizes an automated credit scoring system known as the *Financial Trust Score (FTS).*

4.2 The *FTS* system analyzes financial, behavioral, and device-related data associated with a user in order to generate an automated assessment of the user's creditworthiness.

4.3 Decisions regarding loan approval, loan amount, interest rates, and repayment conditions may be determined automatically by the *FTS* system without direct human intervention.

4.4 Users acknowledge that the precise methodology used to generate the *Financial Trust Score* constitutes proprietary information belonging to *FinCredit Technologies Ltd.*

**5. Sharing of Personal Data**

5.1 *FlashCredit* may share personal data with selected third parties where such sharing is necessary for the operation of the *FlashCredit* platform.

5.2 Such third parties may include:

a) telecommunications service providers that facilitate mobile payment services;
b) data analytics providers engaged in credit risk modelling;
c) credit reference bureaus participating in regional credit information exchange systems;
d) cloud infrastructure providers supporting the operation of *FlashCredit* services.

5.3 *FlashCredit* may also disclose personal data where required by applicable law or regulatory authorities.

**6. Cross-Border Data Processing**

6.1 Personal data collected through the *FlashCredit* platform may be transferred to and processed in jurisdictions outside the *East African Community*.

6.2 Such transfers may occur where *FlashCredit* engages third-party service providers or cloud infrastructure providers located in other jurisdictions.

6.3 *FlashCredit* takes reasonable measures to ensure that such processing is conducted in accordance with applicable data protection standards.

**7. User Consent**

7.1 By selecting the *"I Agree"* option during installation of the *FlashCredit* application, users consent to the collection and processing of personal data as described in this Agreement.

7.2 Users who decline to grant the permissions required for operation of the *FlashCredit* application will be unable to access *FlashCredit* lending services.

**8. Data Security**

8.1 *FlashCredit* implements technical and organizational measures designed to protect personal data against unauthorized access, disclosure, alteration, or destruction.

8.2 Such measures include encryption technologies, authentication protocols, and monitoring systems intended to safeguard the integrity of the *FlashCredit* platform.

**9. Data Retention**

9.1 Personal data may be retained for as long as necessary to provide services through the *FlashCredit* platform and to comply with legal and regulatory obligations.

9.2 *FlashCredit* may retain certain data for longer periods where required for fraud detection, credit risk modelling, or regulatory reporting.

**Annex B: Example of Automated Repayment Reminder Message Sent to Borrower Contacts**

The following text message was reported by several individuals listed in the mobile phone contact list of *Amani Kato* after his failure to repay a digital loan obtained through the *FlashCredit* platform.

The message was generated automatically by the *FlashCredit* repayment notification system and delivered via the mobile telecommunications network operated by *Telelink Communications Plc*.

**Sender:** FlashCredit Alerts
**Delivery Channel:** SMS (Short Message Service)
**Date:** 18 April 2024
**Time:** 09:42 AM

**Message Content:**

*FlashCredit* Notification

Your contact *AMANI KATO* currently has an outstanding loan with *FlashCredit* that is overdue.

Kindly remind them to settle their loan balance as soon as possible to avoid additional penalties.

Thank you for helping maintain responsible borrowing.

FlashCredit Customer Recovery Unit

**Additional System Information (as recorded in *FlashCredit* internal logs):**

- Notification Type: Automated repayment reminder
- Trigger Event: Loan repayment overdue beyond scheduled repayment date
- Recipient Source: Contact list retrieved from borrower's mobile device during application installation
- Delivery Method: SMS gateway integrated with Telelink Communications network
- Message Format: Automated template generated by FlashCredit debt recovery system

**Note:**
According to *FinCredit Technologies Ltd*, the above message forms part of an automated notification mechanism designed to encourage repayment of overdue loans. The company maintains that such notifications are generated by the system when a borrower fails to meet repayment deadlines.

The *Applicants* dispute the legality of this practice and contend that they did not authorize the disclosure of information regarding their loan status to third parties contained in their personal contact lists.

**Annex C: Summary of the cybersecurity researchers' report concerning the exposed database**.

**Digital Security Observatory**

**Preliminary Technical Assessment Report**

**FlashCredit Data Exposure Incident**

**June 2024**

**1. Background of the Investigation**

1.1 In *May 2024*, researchers affiliated with the *Digital Security Observatory (DSO)* began conducting an independent assessment of publicly accessible cloud infrastructure associated with digital financial service providers operating within the *East African region*.

1.2 During the course of this assessment, the researchers identified a cloud-hosted database instance believed to be connected to data processing activities associated with the *FlashCredit digital lending platform*, operated by *FinCredit Technologies Ltd.*

1.3 The database was hosted on cloud infrastructure linked to *DataMind Analytics Ltd*, a third-party analytics provider contracted by *FinCredit* to process borrower data used in automated credit scoring.

**2. Nature of the Vulnerability**

2.1 The researchers determined that the database had been exposed through a *misconfigured Application Programming Interface (API)* endpoint.

2.2 The configuration of the *API* allowed external connections without authentication credentials.

2.3 As a result, the database could be queried through standard web requests without the need for authorized access tokens or password authentication.

2.4 According to the researchers, the configuration error appeared to have occurred within a *cloud-based analytics environment used for credit-scoring data processing.*

2.5 The exposed database appeared to function as an intermediary storage system used for machine-learning analysis related to the *Financial Trust Score (FTS)* algorithm employed by the *FlashCredit* platform.

**3. Categories of Data Identified**

3.1 Based on the researchers' examination of the database structure, the exposed dataset appeared to contain records relating to approximately *500,000 FlashCredit borrowers* across several states within the *East African region.*

3.2 The database fields examined by the researchers indicated the presence of several categories of personal and transactional data.

3.3 The data fields identified included, inter alia:

- borrower mobile phone numbers
- national identification numbers
- loan application records
- repayment histories

- device identifiers linked to borrower accounts
- summarized mobile money transaction records
- internal borrower identification codes used by the FlashCredit platform.

3.4 The researchers indicated that the dataset structure suggested integration between *FlashCredit* user accounts and mobile money transaction metadata associated with the *T-Money* platform operated by *Telelink Communications Plc.*

**4. Duration of Exposure**

4.1 The researchers were unable to determine the exact date on which the database became publicly accessible.

4.2 However, system logs examined during the investigation suggested that the server configuration may have been active for several weeks prior to its discovery.

4.3 The report noted that the cloud infrastructure appeared to be configured using automated deployment tools associated with data-analytics environments.

4.4 The researchers indicated that they could not determine whether any unauthorized third parties had accessed or downloaded the exposed data prior to its discovery.

**5. Notification to the Platform Operators**

5.1 Following confirmation of the exposure, the researchers reported the vulnerability to *FinCredit Technologies Ltd* through a responsible disclosure communication.

5.2 The notification was sent through the company's publicly listed cybersecurity contact channel.

5.3 According to the researchers, the exposed database was subsequently secured within *forty-eight (48) hours* of the notification being sent.

5.4 The researchers did not receive confirmation regarding whether *FinCredit* had conducted a full forensic investigation concerning the incident.

**6. Potential Risks Identified**

6.1 The researchers noted that the exposed dataset contained several categories of information that could potentially allow identification of individual borrowers.

6.2 In particular, the presence of phone numbers, national identification numbers, and device identifiers could allow third parties to associate specific individuals with borrowing activity on the *FlashCredit platform*.

6.3 The report also observed that the inclusion of transaction summaries and repayment histories could allow external actors to infer aspects of an individual's financial behavior.

6.4 The researchers indicated that such data could potentially be used for purposes including:

- identity fraud
- social engineering attacks
- targeted financial scams
- unauthorized profiling of individuals.

**7. Statements from FinCredit**

7.1 Following media inquiries regarding the incident, *FinCredit Technologies Ltd* issued a public statement addressing the reported exposure.

7.2 The company stated that the exposed database belonged to a third-party analytics contractor responsible for data analysis used in credit scoring.

7.3 *FinCredit* further stated that the database did not contain login credentials, payment authorization tokens, or access to active financial accounts.

7.4 According to the company, the exposure did not affect the operational security of the *FlashCredit* platform's lending system.

7.5 The company did not publicly disclose the total number of individuals whose records may have been included in the dataset.

## 8. Recommendations of the Researchers

8.1 The *Digital Security Observatory* recommended that operators of digital financial platforms adopt stronger safeguards for the storage and processing of borrower data.

8.2 The researchers suggested that cloud-based analytics systems used in financial technology services should implement:

- strict authentication controls
- encrypted storage of personal data
- regular configuration audits of cloud infrastructure
- stronger internal oversight of third-party data processors.

8.3 The researchers also recommended that individuals whose data may have been included in the exposed dataset take precautionary measures to reduce potential risks of identity misuse.

## 9. Status of the Investigation

9.1 At the time this summary was prepared, the *Digital Security Observatory* indicated that its investigation had been limited to the identification and disclosure of the exposed database.

9.2 The researchers stated that they had not conducted a forensic investigation to determine whether unauthorized access had occurred.

9.3 The extent to which the exposed data may have been accessed or copied by third parties therefore remains unknown.

## Annex D: Excerpt from the Commercial Data-Sharing Agreement between FinCredit Technologies Ltd and Telelink Communications Plc

### DATA SHARING AND ANALYTICS AGREEMENT

This excerpt is taken from the Commercial Data Integration and Analytics Agreement concluded between *FinCredit Technologies Ltd* and *Telelink Communications Plc* on *12 March 2023*.

### Article 1

### Purpose of the Agreement

1.1 The purpose of this Agreement is to establish a framework under which *Telelink Communications Plc ("Telelink")* shall provide certain categories of telecommunications and mobile financial transaction data to *FinCredit Technologies Ltd ("FinCredit")* for the purpose of supporting the operation of FinCredit's digital lending platform known as *FlashCredit*.

1.2 The Parties acknowledge that the *FlashCredit* platform relies on automated credit-scoring systems that utilize behavioral and financial indicators derived from digital transaction records.

1.3 *Telelink* agrees to provide specified data elements generated through the *T-Money mobile financial services platform* in order to enable *FinCredit* to perform credit risk assessments and fraud detection functions.

### Article 2

### Categories of Data Shared

2.1 Subject to the terms of this Agreement, *Telelink* shall provide *FinCredit* with access to the following categories of data associated with users of the *T-Money* platform:

a. transaction metadata relating to mobile money transfers conducted through *T-Money* accounts;
b. records of account activity, including frequency and volume of transactions;
c. subscriber identity information associated with *T-Money* accounts, including registered phone numbers;
d. mobile device identifiers associated with subscriber accounts;
e. device usage indicators generated through interaction with the *T-Money* platform.

2.2 *Telelink* represents that the data provided under this Agreement shall consist of transactional and technical metadata generated in the course of providing telecommunications and mobile financial services.

2.3 *Telelink* further represents that, where possible, the data shared with *FinCredit* shall be processed through data minimization and pseudonymization techniques prior to transmission.

**Article 3**

**Use of Shared Data**

3.1 *FinCredit* may process the data received from *Telelink* solely for purposes related to:

a. automated credit scoring;
b. fraud detection and risk management;
c. verification of user identity associated with *FlashCredit* accounts;
d. improvement of predictive models used in the *Financial Trust Score (FTS)* algorithm.

3.2 *FinCredit* shall not use the data obtained under this Agreement for purposes unrelated to the operation of the *FlashCredit* lending platform without the prior written consent of *Telelink*.

3.3 *FinCredit* may combine the data received under this Agreement with other categories of user data obtained through the *FlashCredit* application, including device data, behavioral indicators, and data obtained from third-party analytics providers.

**Article 4**

**Data Processing and Cross-Border Transfers**

4.1 *FinCredit* may process data obtained under this Agreement through cloud-based infrastructure operated by its contracted analytics provider, *DataMind Analytics Ltd*.

4.2 Such processing may involve the transfer of data to data centers located outside the territory of the *Republic of Kisiwa*.

4.3 *FinCredit* shall ensure that appropriate technical and organizational measures are implemented to safeguard the security of the data during processing and transmission.

**Article 5**

**Responsibility and Liability**

5.1 Each Party shall remain responsible for the lawful collection of personal data obtained through its respective services.

5.2 *Telelink* represents that subscriber data shared with *FinCredit* has been collected in accordance with applicable telecommunications and financial services regulations.

5.3 *FinCredit* shall bear responsibility for ensuring that the processing of data received under this Agreement complies with applicable data protection and privacy regulations governing digital financial services.

**Article 6**

**Confidentiality**

6.1 The Parties agree that all data exchanged under this Agreement shall be treated as confidential commercial information.

6.2 Neither Party shall disclose such information to third parties except where necessary for the performance of the services described in this Agreement or where required by law.

**Article 7**

**Duration of Agreement**

7.1 This Agreement shall remain in force for an initial period of *three (3) years* from the date of signature.

7.2 The Agreement may be renewed upon written agreement of the Parties.

**Executed on 12 March 2023**

**For FinCredit Technologies Ltd**
Chief Technology Officer

**For Telelink Communications Plc**
Director of Digital Financial Services

**Annex E: Decision of the Kisiwa Data Protection Authority**

**Kisiwa Data Protection Authority (KDPA)**
Office of the Data Commissioner
Republic of Kisiwa

**Decision No. KDPA/INV/07/2025**

**In the matter of:** A complaint concerning the processing of personal data by *FinCredit Technologies Ltd* and *Telelink Communications Plc*

**Complainants:**
Amani Kato
Grace Namugenyi
David Mwangi
Digital Rights Centre

**Respondents:**
FinCredit Technologies Ltd
Telelink Communications Plc

**Date of Decision:** 15 January 2025

## I. Introduction

1. On *12 August 2024*, the *Kisiwa Data Protection Authority (KDPA)* received a complaint submitted jointly by the Complainants concerning the alleged unlawful collection, processing, and disclosure of personal data in connection with the *FlashCredit* digital lending platform.

2. The complaint alleged that the *Respondents* engaged in data processing practices inconsistent with the data protection and privacy laws of the *Republic of Kisiwa.*

3. In particular, the Complainants alleged that *FinCredit Technologies Ltd* and *Telelink Communications Plc* processed personal data without lawful basis, collected excessive categories of personal information, shared such information with third parties without authorization, and failed to implement adequate security safeguards.

4. Pursuant to its statutory mandate under the *Data Protection and Privacy Act of Kisiwa*, the Authority initiated an administrative inquiry into the allegations raised in the complaint.

## II. Issues Considered by the Authority

5. In conducting its review, the Authority considered the following questions:

    i. whether the *FlashCredit* application collected personal data from users in a manner inconsistent with applicable data protection principles;
    ii. whether the *Respondents* obtained valid consent for the collection and processing of such personal data;
    iii. whether the sharing of data between *Telelink Communications Plc* and *FinCredit Technologies Ltd* complied with applicable legal requirements;
    iv. whether the *Respondents* implemented appropriate technical and organizational measures to safeguard personal data against unauthorized access.

## III. Submissions of the Parties

### A. Submissions of the Complainants

6. The *Complainants* submitted that the *FlashCredit* mobile application required users to grant access to multiple categories of personal data stored on their mobile devices, including *contact lists*, *SMS metadata*, *device identifiers*, and *mobile money transaction records*.

7. The *Complainants* argued that many of these categories of data were not necessary for the provision of digital lending services and therefore constituted excessive data collection.

8. The *Complainants* further alleged that users were required to accept a lengthy privacy policy as a condition of accessing the service and that such consent could not be regarded as freely given.

9. The *Complainants* also alleged that *Telelink Communications Plc* had shared subscriber transaction data and mobile account information with *FinCredit* pursuant to a commercial data-sharing agreement that had not been adequately disclosed to subscribers.

10. In addition, the *Complainants* referred to the data exposure incident reported in *June 2024*, arguing that the alleged exposure of borrower records demonstrated inadequate data security practices.

### B. Submissions of the Respondents

*11.* *FinCredit Technologies Ltd* submitted that the data collected through the *FlashCredit* application was necessary for the operation of automated credit scoring systems used to evaluate borrower risk.

12. The *Respondent* argued that the use of behavioral and transactional data constituted a common practice within digital lending models designed to provide financial services to individuals without traditional credit histories.

13. *FinCredit* further submitted that users were informed of the categories of data collected through the *FlashCredit* Privacy and Data Use Agreement, which was made available during the installation process of the application.

14. *Telelink Communications Plc* submitted that the data shared with *FinCredit* consisted of transaction-related metadata associated with the *T-Money* platform and that such sharing occurred pursuant to a lawful commercial integration agreement.

15. *Telelink* also argued that the data exchanged between the parties was necessary to facilitate credit risk analysis and fraud prevention mechanisms within the *FlashCredit* platform.

16. With respect to the reported data exposure incident, *FinCredit* stated that the affected database belonged to a third-party analytics contractor and that remedial steps had been taken to secure the relevant infrastructure.

## IV. Findings of the Authority

17. The *Authority* notes that users of the *FlashCredit* platform were required to accept the *FlashCredit* Privacy and Data Use Agreement as part of the application installation process.

18. The *Authority* further observes that the policy indicates that certain categories of personal data may be collected and processed for purposes including *credit scoring*, *fraud detection*, and *risk management*.

19. The *Authority* recognizes that digital lending platforms frequently rely on automated analysis of behavioral and transactional data in order to evaluate borrower creditworthiness.

20. Based on the information available during the investigation, the *Authority* finds that the categories of data processed by *FinCredit* appear consistent with data practices commonly used within the digital lending sector.

21. With respect to the data-sharing arrangement between *FinCredit Technologies Ltd* and *Telelink Communications Plc*, the *Authority* notes that the parties entered into a commercial agreement facilitating the exchange of certain categories of transaction-related data.

22. The *Authority* considers that such exchanges may form part of the operational integration between mobile financial services and digital lending platforms.

23. Regarding the reported exposure of borrower records, the *Authority* notes that the affected infrastructure was operated by a third-party analytics contractor engaged by *FinCredit*.

24. The *Authority* further notes that the available information does not indicate that payment systems or financial accounts associated with *FlashCredit* users were compromised.

25. The *Authority* also observes that certain elements of the data processing associated with the *FlashCredit* platform were conducted through cloud infrastructure located outside the *Republic of Kisiwa*.

26. Insofar as those processing activities occurred outside the territorial jurisdiction of the *Authority*, they fall beyond the direct enforcement powers of the *KDPA*.

## V. Decision

27. Having considered the submissions of the parties and the information available during the investigation, the *Authority* concludes that the evidence presented does not establish a violation of the data protection obligations applicable under the laws of the *Republic of Kisiwa*.

28. The *Authority* therefore determines that the complaint submitted by the *Complainants* does not warrant further enforcement action.

29. The complaint is accordingly *dismissed*.

**Issued by:**

Kisiwa Data Protection Authority

Office of the Data Commissioner

Republic of Kisiwa

**15 January 2025**

## VII. CLARIFICATIONS

Requests for clarification regarding the facts of the case may be submitted to the Unwanted Witness Privacy Moot Court Competition Secretariat at info@unwantedwitness.org

**The Unwanted Witness**
Bulange, Nsibambi Village P.O.BOX 23184 Kampala – Uganda
Mob: +697635 414-256 Email: info@unwantedwitness.org