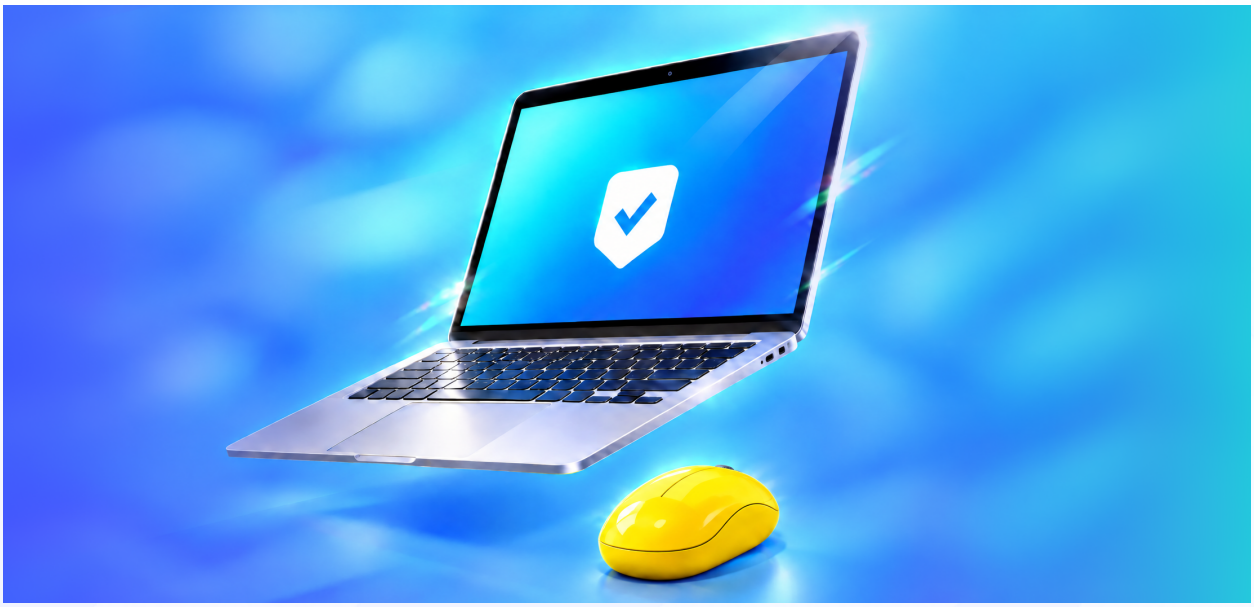
skyro

Closing the Gaps: A Collaborative Framework Against Fraud in the Philippine Digital Lending Ecosystem

Findings and Policy Recommendations from the Philippine Fraud Intelligence Exchange (PH-FIX) Cross-Sector Anti-Fraud Intelligence Roundtable

27 October 2026 | Philippines



Executive Summary

The rapid expansion of digital lending and payment services has created new opportunities for financial inclusion in the Philippines. However, it has also opened new avenues for organized fraud, with criminal networks exploiting legitimate financial products, merchant payment channels, and gaps in coordination between financial institutions.

On 27 October 2026, the Philippine Fraud Intelligence Exchange (PH-FIX) convened a cross-sector Anti-Fraud Intelligence Roundtable, bringing together representatives from government agencies, financial regulators, law enforcement, and the private sector to examine emerging fraud patterns affecting the digital lending ecosystem.

Discussions revealed an important shift in the nature of fraud confronting lenders. Rather than relying exclusively on stolen identities, forged documents, or unauthorized account access, organized groups increasingly exploit legitimate customer onboarding and financing processes. They recruit individuals using their real identities, coach them through loan applications, and subsequently divert financed commodities or credit proceeds for the benefit of organized networks.

Other schemes involve rogue sales agents, fraudulent merchant accounts, social media advertisements, and QR Ph transactions used to convert legitimate credit facilities into cash.

Four recurring vulnerabilities emerged:

1. **Fragmented intelligence:** Individual lenders have limited visibility into fraudulent networks operating across multiple institutions. Recruiters, suspicious merchants, and compromised sales agents can move from one financial institution to another without carrying their fraud history with them.
2. **Limited transaction traceability:** Cash-based arrangements and fragmented payment channels make it difficult to reconstruct the movement of funds and establish the links between recruiters, borrowers, agents, and receiving accounts.
3. **Gaps in institutional coordination:** Financial institutions, regulators, law enforcement, and digital platforms often operate through separate reporting and investigation processes, delaying interventions and allowing fraudulent networks to continue operating.
4. **Evolving fraud methods and legal challenges:** Existing regulatory and enforcement frameworks provide important tools, but questions remain about their application to organized recruitment schemes,

cross-institution intelligence sharing, and fraud involving apparently legitimate transactions.

The roundtable identified the need for a more coordinated approach built around five priorities:

- Establishing a unified industry association or comparable institutional mechanism for fraud prevention and intelligence sharing.
- Developing a legally compliant, cross-sector mechanism for sharing verified fraud indicators.
- Strengthening coordination between lenders, payment service providers, regulators, and law enforcement.
- Improving evidence preservation, scam advertisement takedowns, and the investigation of suspicious merchant accounts.
- Embedding fraud awareness and prevention measures into the customer onboarding and lending journey.

The central proposition of this paper is that **fraud prevention must move beyond institution-level detection toward a coordinated intelligence ecosystem that identifies and disrupts organized networks before they can victimize additional borrowers and financial institutions.**

1. Background and the Evolving Fraud Landscape

Digital lending has become an important component of the Philippines' financial services ecosystem. The availability of online loan applications, point-of-sale financing, digital credit facilities, and interoperable payment systems has made borrowing and financial transactions more accessible.

At the same time, the volume and nature of reported cybercrime highlight the growing importance of stronger consumer and institutional safeguards.

The Cybercrime Investigation and Coordinating Center (CICC) recorded 18,633 cybercrime complaints in 2025, compared with 10,004 in 2024. Of the 2025 complaints, 6,453 involved consumer fraud and 4,243 involved online fraud.

These figures cover broader cybercrime categories and are not limited to online lending. [2]

Separately, the Presidential Anti-Organized Crime Commission reported receiving 47,446 complaints concerning allegedly abusive online lending practices between August 2024 and January 2026. These are reported complaints, not necessarily adjudicated violations or unique confirmed victims. [3]

During the PH-FIX roundtable, CICC also presented figures indicating that it had received more than 8,000 online-lending-related reports between January 2025 and October 2026. According to the presentation, approximately 47% involved online lending fraud and 52.3% involved online harassment. [1]

These figures illustrate two distinct but interconnected challenges: protecting borrowers from abusive lending practices and protecting legitimate financial institutions and their customers from organized fraud.

The latter requires particular attention because fraudulent activity increasingly occurs through transactions that may initially appear legitimate.

1.1 From identity fraud to the exploitation of legitimate transactions

Traditional fraud controls commonly focus on identifying suspicious applicants, detecting falsified documents, validating identity, and monitoring unusual account activity.

However, the schemes presented at the roundtable demonstrate that fraudsters can circumvent these controls by using genuine borrower identities and authentic application information.

In several instances, customers willingly participate in recruitment arrangements, either because they are promised small cash incentives or because recruiters misrepresent the nature of the transaction. The resulting loan may be properly documented and approved, even though the underlying economic arrangement is fraudulent.

This creates a difficult situation for financial institutions. The customer may have completed the application and received the financed commodity or credit facility, but the benefit of the transaction is ultimately diverted to a third party.

The fraud therefore occurs not necessarily in the application itself, but in the recruitment, inducement, diversion, and subsequent conversion of the proceeds.

2. Emerging Fraud Typologies

The following typologies consolidate the anonymized cases and patterns discussed during the roundtable. They illustrate recurring methods and vulnerabilities rather than findings against any particular institution or individual.

2.1 Organized borrower recruitment and financed-goods conversion

Organized recruiters approach individuals in residential communities and other accessible locations, offering cash incentives in exchange for using their identities to obtain financing.

Applicants are typically instructed to use their genuine identification documents and personal information. Recruiters may also coach them on how to respond to questions from sales agents or credit assessors.

After loan approval, the financed commodity is exchanged for cash outside the participating merchant's premises. The recruiter takes possession of the commodity or its proceeds, while the borrower remains legally responsible for the loan.

In some cases, borrowers are assured that they will not need to make repayments or are instructed to ignore subsequent communications from the lender.

The scheme presents several challenges:

- Applications may pass conventional identity verification because the applicant's information is genuine.
- The transaction may appear legitimate from the merchant's perspective.
- Cash handovers outside the merchant premises create a limited digital payment trail.
- The same recruitment network may target several lenders within a short period, potentially before overdue borrowing information is updated across the industry.

Key vulnerability: Individual lenders have limited visibility into coordinated recruitment activity occurring across competing institutions.

2.2 Insider-assisted fraud and credit-line diversion

Another pattern involves sales personnel or agents colluding with external recruiters to obtain access to customers' credit facilities.

Customers are offered small cash incentives in exchange for using their identities to secure a credit line. The available credit is then used to initiate payments through QR Ph merchant accounts or other payment channels.

The funds may subsequently be converted into cash through receiving merchants or electronic wallets, with the proceeds diverted to the perpetrators.

In some instances, customers may not fully understand that they have incurred a loan obligation, only discovering the consequences when payments become due.

The problem extends beyond the initial transaction. When compromised agents are terminated, they may seek employment with other lenders, allowing the same fraudulent practices to recur.

Key vulnerabilities:

- No established cross-institution mechanism for sharing verified information about agents involved in fraud.
- Limited visibility into potentially suspicious receiving merchants and QR transaction patterns.
- Difficulties obtaining transaction and account information across different payment providers.
- Inconsistent processes for escalating suspected internal fraud to other institutions.

2.3 Fraudulent advertisements offering credit-to-cash conversion

Fraudulent groups use social media advertisements and messaging applications to offer borrowers the ability to convert existing credit lines or approved financing into cash.

Customers are instructed to complete a transaction through a merchant account or QR Ph code. After the payment is made, the supposed intermediary disappears, leaving the customer with an outstanding loan obligation and no corresponding cash benefit.

These schemes exploit the legitimate use of digital payment infrastructure to facilitate fraudulent transactions.

Fraudulent advertisements and group chats may be removed or abandoned once complaints emerge, only for similar advertisements and accounts to reappear under different identities.

Key vulnerabilities:

- Limited coordination between lenders and digital platforms for rapid identification and removal of fraudulent advertisements.
- Delays in identifying and reporting receiving merchant accounts.
- Difficulty preserving evidence from social media posts and private messaging groups before it disappears.

2.4 Product financing conversion through organized intermediaries

A related scheme involves recruiters advertising opportunities to convert product financing into cash.

The recruiter facilitates the application, coaches the borrower through the purchase process, and subsequently takes possession of the financed commodity. The borrower receives only a portion of the commodity's value in cash, while remaining liable for the full financing amount.

For example, a borrower may obtain financing for a product valued at ₱30,000 but receive only approximately ₱15,000 from the recruiter.

From a transaction-processing perspective, the purchase may appear authorized and complete. Establishing the deception may therefore require evidence of the recruiter's representations, the subsequent transfer of the commodity, and the financial arrangement between the parties.

Key vulnerability: Existing fraud controls may not readily detect organized social engineering that takes place outside the digital application or merchant transaction itself.

2.5 Common characteristics across the typologies

Despite their differences, the schemes share several characteristics:

- **Legitimate identities:** Fraudsters frequently exploit authentic identification documents and customer information rather than relying on fabricated identities.
- **Third-party inducement:** Recruiters, agents, or intermediaries influence customers to undertake transactions for someone else's benefit.
- **Fragmented transaction chains:** The application, commodity purchase, QR transaction, and eventual cash conversion may occur through different parties and institutions.

- **Cross-institution activity:** Fraudulent groups can target multiple lenders or change institutional affiliations to avoid established controls.
- **Borrower vulnerability:** Customers may be deceived, financially incentivized, or insufficiently aware of the obligations and risks attached to the transaction.

These characteristics suggest that fraud prevention must account for the broader network surrounding a transaction, rather than focusing exclusively on the identity of the borrower or the legitimacy of the individual transaction.

3. Structural and Regulatory Gaps

The discussions identified several structural issues that limit the industry's ability to detect and respond to organized lending fraud.

3.1 Fragmented intelligence and the absence of shared fraud signals

Fraud intelligence generally remains within individual institutions.

A lender may identify a suspicious recruiter, a compromised sales agent, or a merchant account associated with fraudulent transactions, but other lenders may have no access to these signals.

This creates an opportunity for fraud networks to transfer their activities between institutions.

Existing credit information infrastructure provides an important foundation for responsible lending. Under Republic Act No. 9510, or the Credit Information System Act, covered submitting entities are required to provide positive and negative credit information to the Credit Information Corporation (CIC).

However, credit reporting is not equivalent to real-time fraud intelligence. The Act provides for regular submissions at intervals of not less than 15 and not more than 30 working days. CIC information is also subject to purpose limitations, including the use of credit information to establish borrowers' creditworthiness. [7]

Consequently, the existing system does not fully address the need to identify coordinated applications, suspicious agents, repeat recruiters, and fraudulent merchant accounts in near real time.

3.2 Limited visibility across payment channels

Credit providers frequently depend on banks, e-money issuers, payment service providers, and merchant acquirers to obtain information about transactions and receiving accounts.

A lender may know that a customer used a credit line to make a suspicious QR payment but may not have sufficient information to identify the receiving account holder or trace subsequent transfers.

Republic Act No. 10175, or the Cybercrime Prevention Act of 2012, provides a legal framework for law enforcement authorities to obtain computer data through court-authorized warrants, including a Warrant to Disclose Computer Data (WDCD).

While this framework provides a legitimate avenue for investigation, assembling the required documentary package and securing the relevant warrant can add time to an investigation. [8]

The challenge is particularly significant when funds are transferred rapidly across multiple accounts.

3.3 Insufficient coordination on agent and merchant misconduct

Unlike credit information, which is systematically reported through CIC, there is no equivalent industry-wide mechanism identified during the roundtable for

sharing verified information about sales agents involved in organized fraud.

The same problem applies to merchants and receiving accounts associated with suspicious transactions.

Without a structured mechanism, individual institutions may repeatedly encounter the same fraudulent actors without knowing their previous history.

3.4 Consumer awareness has not kept pace with recruitment schemes

Financial literacy and consumer protection campaigns have traditionally emphasized identifying unauthorized lending applications, avoiding scams, and recognizing abusive collection practices.

These remain important priorities. However, an additional awareness gap has emerged: customers who knowingly submit loan applications but are being manipulated into facilitating fraudulent transactions.

Individuals may not understand that allowing another person to use their identity, obtaining financing for a third party, or transferring the proceeds of a credit facility can expose them to financial and potentially legal consequences.

Awareness initiatives must therefore address not only the risks of borrowing from fraudulent lenders, but also the risks of becoming an unwitting participant in a recruitment or money-muling scheme.

3.5 Legal uncertainty surrounding organized recruitment

The roundtable also raised questions regarding the appropriate legal treatment of organized face-to-face recruitment schemes.

The Anti-Financial Account Scamming Act (AFASA), or Republic Act No. 12010, already criminalizes certain money-muling activities, including recruiting individuals to allow their financial accounts to be used for transactions

involving proceeds of crime. It also penalizes defined social engineering schemes involving deception and unauthorized access to financial accounts.

However, whether particular recruitment arrangements involving valid loan applications and the transfer of financed commodities fall within these provisions depends on the specific conduct, the financial accounts involved, and the elements of the offense.

Not every transaction involving a recruited borrower automatically constitutes money muling or social engineering under AFASA. Other applicable fraud and criminal laws may also need to be considered. [4]

Further legal clarification would help distinguish ordinary borrower misconduct, victimization through deception, and organized criminal recruitment.

4. Existing Government and Regulatory Initiatives

The roundtable highlighted several existing mechanisms that could serve as building blocks for a stronger anti-fraud ecosystem.

4.1 Anti-Financial Account Scamming Act

Republic Act No. 12010, or AFASA, establishes an important framework for preventing, detecting, and responding to financial account-related fraud.

Among its key mechanisms are:

- Criminalization of money-muling activities and defined social engineering schemes.
- Requirements for financial institutions under the jurisdiction of the Bangko Sentral ng Pilipinas (BSP) to maintain appropriate fraud management systems and account-protection controls.
- Temporary holding of funds subject to disputed transactions, within the periods and procedures prescribed by BSP.

- Coordinated verification between institutions involved in disputed transactions.
- Information-sharing mechanisms for financial account investigations involving competent government authorities.

BSP Circular Nos. 1213, 1214, and 1215, Series of 2025, operationalize important aspects of AFASA, including fraud management, investigations, information sharing, and coordinated verification. [4]

One particularly relevant provision is the coordinated verification process. Under Section 8 of AFASA, institutions may initiate verification upon receiving a complaint, information from another institution, or a finding through their fraud management systems.

The law also provides that the Data Privacy Act and specified bank secrecy laws do not apply during this particular coordinated verification process, subject to the safeguards prescribed by the implementing regulations.

This is an important foundation for faster information exchange when suspicious transactions involve multiple institutions.

However, this exemption is limited to the coordinated verification of disputed transactions. It should not be interpreted as blanket authority to create an unrestricted, industry-wide database of suspected borrowers, agents, recruiters, or merchants.

The scope of AFASA must also be carefully considered because the Act defines covered institutions by reference to BSP jurisdiction. The position of SEC-regulated financing and lending companies must therefore be assessed separately.

4.2 Data privacy and the role of the National Privacy Commission

The Data Privacy Act of 2012 (Republic Act No. 10173) does not prohibit all forms of information sharing for fraud prevention.

Section 12 recognizes several lawful bases for processing personal information, including consent, contractual necessity, legal obligation, public authority functions, and legitimate interests, subject to the conditions prescribed by law.

The Act also imposes general requirements of transparency, legitimate purpose, proportionality, accuracy, security, and appropriate retention. Processing sensitive personal information is subject to additional restrictions under Section 13. [5]

The Act's investigation-related provision under Section 19 is not a general exemption from privacy obligations. Its text specifically addresses the non-applicability of the immediately preceding data-subject rights provisions to personal information gathered for investigations involving criminal, administrative, or tax liabilities.

The National Privacy Commission (NPC) has also issued rules on data-sharing agreements and the processing of personal information for loan-related transactions.

Importantly, in March 2026, the NPC, SEC, and DICT jointly reiterated that unnecessary access to borrowers' contact lists and their disproportionate use for debt collection, harassment, or public shaming are prohibited. [6]

The NPC should therefore be involved in designing any proposed fraud intelligence-sharing mechanism to ensure that it has an appropriate legal basis and adequate safeguards.

4.3 Securities and Exchange Commission

The SEC has established rules governing financing and lending companies, including restrictions on unfair collection practices under Memorandum Circular No. 18, Series of 2019.

The circular prohibits harassment, threats, deceptive collection practices, and the unauthorized disclosure of borrower information. It also identifies circumstances in which customer information may be exchanged with other

financial institutions, credit information bureaus, and lenders. [6]

In July 2026, the SEC issued Memorandum Circular No. 20, Series of 2026, prescribing updated prudential, disclosure, and market conduct requirements for financing and lending companies, while lifting the moratorium on online lending platforms. The SEC's published register of recorded online lending platforms provides an additional reference for verifying regulated providers. [9]

These measures are relevant to the broader effort to strengthen accountability and distinguish legitimate lending operations from unauthorized or abusive operators.

4.4 Cybercrime Investigation and Coordinating Center

CICC plays a potentially significant role as a convening and coordination institution.

During the roundtable, CICC expressed willingness to support an organized industry association through threat-monitoring tools, training, and access to its threat monitoring capabilities.

It also proposed exploring a data-fusion repository that could bring together digital evidence, financial tracking information, and reports from relevant government agencies.

Such an arrangement could reduce fragmentation and allow authorities to identify relationships between apparently unrelated fraud incidents.

4.5 Law enforcement coordination

The PNP Anti-Cybercrime Group emphasized the importance of complete documentary submissions when requesting warrants to disclose computer data.

A more standardized evidentiary package from lenders and payment providers could help law enforcement assess cases more efficiently and

minimize repeated requests for supporting documents.

The roundtable also highlighted the value of closer coordination between law enforcement and payment institutions when identifying and tracing suspicious receiving accounts.

5. Policy Recommendations

The following recommendations translate the roundtable's discussions into an industry-level action agenda.

Recommendation 1: Establish a unified industry association or dedicated anti-fraud consortium

The industry should explore the formation of a single, organized association of legitimate online lending and financing providers, with a defined mandate covering fraud prevention, intelligence sharing, and consumer protection.

A unified body would provide government agencies with a consistent institutional counterpart and reduce the fragmentation associated with individual company-to-agency engagements.

Its core functions should include:

- Establishing common fraud taxonomies, reporting standards, and minimum evidence requirements.
- Maintaining an industry-wide channel for communicating emerging fraud patterns.
- Coordinating referrals and intelligence-sharing initiatives with CICC, SEC, BSP, NPC, and law enforcement.
- Facilitating training, threat briefings, and coordinated industry responses.
- Establishing membership standards and a code of conduct that reinforces responsible lending and consumer protection.

Payment service providers and other relevant financial institutions should be invited to participate in appropriate working groups.

CICC's offer of technical support, training, and threat-monitoring access provides a practical starting point for institutionalizing this collaboration.

Recommendation 2: Develop a legally compliant cross-institution fraud intelligence-sharing mechanism

The industry should work with the relevant regulators to establish a structured mechanism for exchanging fraud indicators.

The initial scope should focus on information that helps institutions identify organized networks, including:

- Verified indicators associated with fraudulent recruiters and intermediaries.
- Sales agents with substantiated involvement in organized fraud.
- Merchant and payment-account identifiers associated with confirmed or credibly documented fraudulent transactions.
- Repeated transaction patterns and emerging recruitment methods.
- Relevant digital identifiers and evidence that can link related incidents.

Rather than immediately creating an unrestricted blacklist, the mechanism should adopt a tiered approach:

Level 1 – General threat intelligence: Aggregated and anonymized information on fraud patterns, emerging schemes, and common indicators.

Level 2 – Restricted fraud indicators: Risk signals and identifiers shared through an appropriately governed and legally authorized mechanism, with defined access and permitted uses.

Level 3 – Case-specific investigative information: Identifiable account, customer, transaction, or personal information shared through applicable

legal channels, including AFASA mechanisms and authorized law enforcement processes.

The framework should establish clear standards for accuracy, source verification, data minimization, access controls, retention, audit trails, correction of inaccurate information, and safeguards against malicious or unwarranted reporting.

Importantly, a customer who has been recruited or deceived should not automatically be classified as a fraud perpetrator. The system must distinguish between victims, potentially exploited account holders, and individuals with substantiated involvement in organized fraud.

The NPC should be consulted before implementation to determine the appropriate legal bases, data-sharing arrangements, and safeguards. Consent may be one lawful basis in appropriate circumstances, but a blanket consent requirement tied to access to credit should not be assumed to resolve all privacy issues.

Recommendation 3: Strengthen the reporting and tracing of suspicious QR Ph merchants

Financial institutions should establish a more coordinated process for identifying and reporting merchant accounts associated with suspicious QR transactions.

Where a disputed payment has taken place, the customer and relevant lender should promptly notify the issuing bank or e-money provider.

The institution handling the payment can assess whether the transaction qualifies for the AFASA temporary-holding and coordinated-verification processes, and whether escalation to law enforcement is warranted.

The industry should also work with BSP and relevant payment system stakeholders on improving merchant identification and risk monitoring.

This may include:

- More consistent use of merchant identifiers and merchant category information.
- Improved monitoring of unusual merchant transaction velocity and patterns.
- Faster referral of suspicious merchants to the relevant acquiring or issuing institutions.
- Clearer procedures for preserving transaction references and supporting documentation.

The roundtable also discussed proposed improvements in QR merchant data infrastructure and the use of merchant category codes. Their specific scope, regulatory status, and implementation timelines should be confirmed with BSP.

Recommendation 4: Establish a common evidence-preservation and scam takedown protocol

Speed is critical when dealing with online advertisements, messaging groups, and fraudulent social media accounts.

The industry should coordinate with CICC and relevant platforms to develop a standardized reporting process for suspected credit-conversion scams and fraudulent recruitment advertisements.

At a minimum, reports should preserve:

- Screenshots of advertisements and relevant conversations.
- Original URLs, account names, page identifiers, and group information.
- Dates and timestamps of relevant interactions.
- QR codes, merchant identifiers, and transaction reference numbers.

- Relevant payment receipts and supporting customer documentation.

Lenders should also encourage customers to submit screenshots of suspicious advertisements and group conversations through secure reporting channels.

The objective should be to move from isolated takedown requests toward coordinated identification of related accounts, pages, advertisements, and receiving payment channels.

Because perpetrators can quickly create replacement accounts, enforcement should focus on disrupting the underlying networks rather than removing individual advertisements alone.

Recommendation 5: Introduce industry-wide standards for agent fraud prevention

The mobility of fraudulent sales agents between institutions creates a particular risk.

The industry should explore standardized internal controls and a mechanism for sharing verified misconduct signals through an appropriate legal and privacy framework.

Measures may include:

- Standardized agent identification and accreditation.
- Clear documentation of termination arising from substantiated fraud or serious misconduct.
- Enhanced background and reference verification when onboarding agents with prior relevant employment.
- Periodic reviews of agent productivity and unusual transaction patterns.
- Stronger monitoring of applications involving unusual referral or recruitment behavior.

Any shared information about employees or former agents should be subject to validation, appropriate access restrictions, and a process for correcting disputed information.

The objective is to prevent repeat offenders from exploiting gaps between employers without creating an indiscriminate employment blacklist.

Recommendation 6: Embed fraud awareness into the customer onboarding journey

Fraud prevention should not be limited to periodic marketing campaigns or customer service advisories.

Lenders should integrate short, clear, and recurring awareness materials into their application, approval, and disbursement processes.

These should explain that:

- Borrowers remain responsible for loans obtained using their identities, even when another person promises to make the payments.
- Customers should never allow another person to use their identity or financial account in exchange for cash incentives.
- Financing proceeds and credit facilities should not be transferred to unauthorized intermediaries.
- Offers to convert loans or credit lines into cash through unofficial channels are potential scams.
- Customers should verify the identity of agents and merchants and report suspicious recruitment activities immediately.

Particular attention should be given to individuals who may be recruited into these schemes without understanding the financial and legal consequences.

A simple knowledge check before disbursement may also help ensure that borrowers understand the transaction they are entering into.

Recommendation 7: Pursue regulatory clarification and stronger legal coordination

The industry should engage regulators and law enforcement on the following outstanding issues:

Data-sharing authority. Seek NPC guidance on the legal bases and safeguards for sharing fraud indicators among SEC-regulated lending and financing companies, banks, and payment providers.

AFASA participation. Engage BSP on the eligibility of non-bank lenders, particularly SEC-regulated financing and lending companies, to participate in applicable AFASA information-sharing and coordinated-verification processes.

FI-initiated escalation. Clarify the circumstances under which financial institutions may initiate AFASA requests or referrals based on internally detected fraud, without waiting for an individual account-holder complaint.

Organized recruitment schemes. Request a legal assessment of recruitment arrangements involving apparently valid loan applications, deceptive inducement, and subsequent diversion of financed commodities or proceeds.

Evidence and warrants. Work with PNP-ACG to standardize documentary requirements for WDCD applications and other investigative requests, including those involving QR Ph merchants and receiving accounts.

Cross-border enforcement. Strengthen coordination mechanisms for cases involving recruiters, administrators, or beneficiaries operating outside Philippine jurisdiction.

These engagements should aim to clarify the application of existing laws before pursuing new legislation, while identifying genuine gaps that may require regulatory or legislative intervention.

6. Proposed Implementation Roadmap

To translate these recommendations into measurable outcomes, the following phased approach is proposed.

Timeline	Priority actions	Expected outputs
0–3 months	Organize a unified industry working group; establish CICC and regulatory engagement channels; agree on common fraud typologies and evidence requirements; begin customer awareness initiatives.	Industry governance structure, initial fraud taxonomy, standardized reporting template, borrower awareness materials.
3–6 months	Consult NPC on data-sharing arrangements; engage BSP and SEC on AFASA participation and referral mechanisms; pilot structured information exchange for verified fraud cases.	Proposed data-sharing framework, agency referral protocol, pilot intelligence-sharing mechanism.
6–12 months	Operationalize the industry fraud intelligence mechanism; establish regular threat briefings and coordinated reporting with CICC; assess the feasibility of a government-supported data-fusion platform.	Operational intelligence mechanism, recurring threat reports, improved case coordination and monitoring.

Suggested performance indicators

The effectiveness of the proposed initiatives should be assessed using measurable indicators, including:

- Number of participating institutions in the unified industry mechanism.
- Number of verified fraud indicators and related incidents shared.
- Average time between fraud reporting and institutional action.
- Average time required to identify and escalate suspicious merchant accounts.
- Number of fraudulent advertisements or accounts successfully referred for takedown.
- Number of repeat fraud incidents linked to previously identified agents, recruiters, or merchants.
- Estimated losses prevented and funds successfully recovered.
- False-positive rates and the number of disputed or corrected fraud indicators.

These metrics should be reviewed periodically to ensure that stronger fraud controls do not come at the expense of legitimate borrowers' access to financial services.

7. Conclusion: From Fragmented Responses to Collective Action

The discussions at PH-FIX demonstrate that organized lending fraud cannot be addressed by individual financial institutions acting independently.

Fraud networks operate across institutional boundaries. They exploit legitimate customer identities, sales channels, financing products, merchant accounts, and payment infrastructure. They adapt quickly when one institution strengthens its controls, often moving to another provider or channel.

The industry's response must therefore become equally coordinated.

The Philippines already has important foundations in place: AFASA provides stronger financial-account protection and coordination mechanisms; the

Data Privacy Act provides a framework for responsible data processing and sharing; the SEC and NPC have established consumer protection rules; and agencies such as CICC and PNP-ACG provide avenues for intelligence coordination and enforcement.

The opportunity now is to connect these mechanisms into a more coherent system.

A unified industry association, a legally sound fraud intelligence-sharing framework, stronger payment traceability, coordinated law enforcement engagement, and proactive customer education can collectively reduce the ability of organized fraud networks to operate across the financial ecosystem.

Ultimately, the goal is not simply to reduce fraud losses incurred by individual institutions. It is to protect Filipino consumers, preserve confidence in legitimate digital financial services, and ensure that the continued expansion of financial inclusion is not undermined by increasingly organized criminal activity.

Fraud is a shared risk. Its prevention must be a shared responsibility.

References

[1] Event material. CICC presentation and discussions during the Philippine Fraud Intelligence Exchange (PH-FIX) Cross-Sector Anti-Fraud Intelligence Roundtable, 27 October 2026. The online-lending-specific figures should be reconfirmed with CICC before publication.

[2] CICC nationwide cybercrime statistics. GMA Integrated News, *Consumer fraud topped complaints logged among senior citizens in 2025 — CICC*, 24 February 2026.

https://www.gmanetwork.com/news/topstories/nation/977680/consumer-fraud-topped-complaints-logged-among-senior-citizens-in-2025-cicc/story/

[3] Online lending complaints. Inquirer.net, *Over 47,400 complaints logged vs abusive online lending apps since 2024*, 16 March 2026.

https://newsinfo.inquirer.net/2196459/over-47400-complaints-vs-abuses-by-online-lending-apps-since-2024-paocc

[4] Anti-Financial Account Scamming Act. Republic Act No. 12010 (2024) and BSP Circular Nos. 1213, 1214, and 1215, Series of 2025.

https://lawphil.net/statutes/repacts/ra2024/ra_12010_2024.html

https://www.bsp.gov.ph/Regulations/Banking%20Laws/AFASA-Booklet-with-IRRs.pdf

[5] Data Privacy Act. Republic Act No. 10173 (2012) and its Implementing Rules and Regulations; NPC Circular No. 2020-03 on Data Sharing Agreements.

https://privacy.gov.ph/data-privacy-act/

https://privacy.gov.ph/implementing-rules-regulations-data-privacy-act-2012/

[6] Online lending consumer protection. NPC Circular No. 20-01, as amended by NPC Circular No. 2022-02; SEC Memorandum Circular No. 18, Series of 2019; Joint DICT-NPC-SEC Public Advisory on Online Lending Platforms, 18 March 2026.

https://privacy.gov.ph/online-lenders-barred-from-harvesting-borrowers-phone-and-social-media-contact-list-says-privacy-commission/

https://lpr.adb.org/sites/default/files/2024-04/philippines-2019-mc-no-18.pdf

https://privacy.gov.ph/wp-content/uploads/2026/03/DICT-NPC-SEC-Public-Advisory-on-Online-Lending-Platforms.pdf

[7] Credit information infrastructure. Republic Act No. 9510, Credit Information System Act; Credit Information Corporation, Submission of Data to the CIC.

https://cic.gov.ph/republic-act-no-9510-credit-information-system-act-cisa/

https://cic.gov.ph/submission-data-cic/

[8] Cybercrime investigation. Republic Act No. 10175, Cybercrime Prevention Act of 2012; Rule on Cybercrime Warrants, A.M. No. 17-11-03-SC.

https://cybercrime.doj.gov.ph/republic-act-no-10175-cybercrime-prevention-act-of-2012/

https://oca.judiciary.gov.ph/wp-content/uploads/A.M.-No.-17-11-03-SC.pdf

[9] SEC regulation of lending and financing companies. SEC Memorandum Circular No. 20, Series of 2026, 7 July 2026; List of Recorded Online Lending Platforms.

https://www.sec.gov.ph/mc-2026/sec-mc-no-20-series-of-2026/

https://www.sec.gov.ph/lending-companies-and-financing-companies-2/list-of-recorded-online-lending-platforms

[10] International reference. Singapore Ministry of Home Affairs, *Measures to Curb Money Mule Activities*, 12 January 2026; Singapore's National Scams List and cross-sector information-sharing initiatives.

https://www.mha.gov.sg/media-room/newsroom/measures-to-curb-money-mule-activities/