THE LEVEL ONE PROJECT

A FRAUD MITIGATION APPROACH FOR INCLUSIVE INSTANT PAYMENTS SYSTEMS

The Level One Project is an initiative of the Gates Foundation

Note to Reader

This 2025 revised version *of A Fraud Mitigation Approach for Inclusive Instant Payment Systems*, has been updated to reflect changes in terminology, based on evolutions in the Instant Payment Landscape and the way the Level One project team describes its work.

For those already familiar with this report, you will notice slight changes in terminology: What we formerly called Fraud Principles, are now 'core tenets' of fraud mitigation. What were once called Best Practices are now termed Guidance.

These changes better reflect how fraud-related content has been integrated within the full set of revised L1P Principles and Practices.

We encourage readers to explore the Level One Project website leveloneproject.org for related guidance.

Meanwhile, the core concepts, examples, and theoretical underpinnings of this report remain fundamentally unchanged.

It is our hope that this report continues to serve as a useful consolidation of fraud-related content to help implementors navigate the evolving nature of fraud threats and mitigation.

Contents

THE LEVEL ONE PROJECT

Section 1

Fraud and Inclusive IPS

1

Applying an Inclusive Lens

As instant payments systems (IPSs) gain traction globally, so do fraudulent payments processed through these systems.

Fraudulent payments are not unique to IPSs. All payments systems and payment methods are targets for fraudsters, particularly as they become more established. Fraud is harmful to the IPS ecosystem and particularly detrimental to low-income and women end users. An Inclusive approach is needed to guide a holistic response to fraud.

The Level One Project

The Level One Project is an initiative of the Gates Foundation's Inclusive Financial Systems (IFS) program. The Level One Project advocates for inclusive, interconnected digital economies to bring poor people into the global financial system, and ultimately to help promote global growth and opportunity.

Working across the public, private, and nonprofit sectors in coordination with a wide variety of institutions, the Level One Project is a multi-year effort to address digital payments system infrastructure at a national and regional level and do so in a way that's both sustainable and compelling for providers of financial services.

Level One Principles

A set of principles to guide countries, regions, or commercial organizations working to create instant payments systems that are inclusive and meet the needs of low-income consumers. Such systems are referred to as **inclusive, instant payments systems (Inclusive IPSs)**. An Inclusive IPS includes a scheme (set of rules that govern participation) and platform (the technology used to operate the system).

Fraud Mitigation Lens

The fraud mitigation lens presented in this report offers a consolidation of essential guidance to help entities enact effective fraud mitigation while preserving a commitment to inclusion. This guidance is also integrated within core level One Principles and Practices.

With increasing and accelerating adoption of L1P aligned inclusive instant payment systems in low- and medium-income countries comes a renewed focus on consumer protection and preventing systemic fraud. We have updated the L1P guide to add a small number of sharp fraud management related tenets, which will increase dramatically the safety of digital payment platforms for users and providers alike.

As always, these additions are the result of intense consultation across the industry. However please do not hesitate to reach out to me and my team with your insights and suggestions.

Kosta Peric

Deputy Director, Payments Infrastructure, Inclusive Financial Systems
Global Growth and Opportunity, Gates Foundation

More Information and glossary of terms: Level One Project Guide

Level One Project Focus

The Level One Project remains focused on enabling financial inclusion by meeting the needs of low-income and women end users—both individuals and merchants—as well as the digital financial service providers (DFSPs) that serve them.

Affordable payments are foundational
to meeting the needs of low-income and women end-users

Affordability

Low Cost

End users are willing and able to pay for the cost of preferred products and receive value in excess of cost

Scale

The cost of the system is spread across a huge volume of payments, making the cost per transaction very low

Safe

Parties in the instant payments ecosystem can use services securely without concern about fraud loss

Usefulness

Reliable

Users' money and information are secure and available for use

Inclusive

Any end user can pay any other end user

Ubiquitous

End users can send and receive payments for all necessary purposes and use cases

Core Tenets of Fraud Mitigation

These fours tenets of fraud mitigation are intended to provide Inclusive IPSs a starting point toward effective fraud mitigation. The report offers example approaches and design guidance to demonstrate how the objectives of each tenet may be pursued.

Inclusive IPSs are well placed to lead the ecosystem toward minimizing the detrimental impact of fraud on end users. Most directly, Inclusive IPSs can achieve this by providing standards and tools to their digital financial service providers (DFSPs) that are designed to help them manage fraud risk while reducing the cost to individual participants.

DFSPs have a direct relationship with end users to whom they provide transaction accounts. This gives impetus for DFSPs to implement fraud risk controls that prevent loss of end user trust and use of services. Clarity that end users are not responsible for financial losses in cases of confirmed fraudulent transactions provides further incentive for DFSPs to manage the risk closely. The ecosystem will be made safer and more inclusive with Inclusive IPSs defining what strong risk management looks like, providing tools to DFSPs, and establishing data guidance.

Tenet 1: Liability

End users are not liable for confirmed fraudulent payments.

Tenet 2: Rules

The Inclusive IPS guides DFSPs in managing fraud risk through their scheme rules.

Tenet 3: Tools

The Inclusive IPS provides fraud mitigation tools and share in the investment.

Tenet 4: Data

The Inclusive IPS establishes fraud data and information-sharing guidelines and mechanisms.

IPS Are Proliferating

As of March 2023, 80+ domestic IPS globally and more in development.

On the African continent alone, in 2022 there were more than 40 domestic IPS in place or in development and in various stages of achieving inclusivity. Since 2018, IPS transaction volumes in Africa have experienced a 32% average annual increase.

We strongly believe in the potential for Africans to power the transformation of the continent. Access to payments systems and transaction accounts via instant payments is the first step for broader financial inclusion and self-empowerment. We recognize the progress to date in launching IPS on the continent and are committed to enabling the journey to full financial inclusion.

Dr. Robert Ochola
Chief Executive Officer
AfricaNenda

Source of map content: The State of Instant and Inclusive Payment Systems (SInclusive IPS) in Africa, 2022. https://www.africanenda.org/en/sInclusive IPS2022

Benefits of *Inclusive* IPS Are Materializing

As more countries and regions implement systems that align with the Level One Principles, the transformation to inclusivity is underway and the benefits of inclusive instant payments systems to end users are coming to fruition.

Benefits of Inclusive IPSs Are Felt in End Users' Lives

You would not have to worry too much about the cash you have on you because everywhere you are, you can easily send the money and it is safe as well.

Despite your location you can still do a transfer and the person can instantly get the money.

—

End Users, Ghana

Quotes from AfricaNenda Consumer Research Insights

We only have the digital option. Someone may need money urgently for hospital; for that Google Pay or PhonePe will be useful. If a friend calls and says my mother is in the hospital, I need 10,000, we can send it immediately. At midnight no banks or anything will be there. We should use digital, but carefully.

—

End User, India

Quote from BMGF-sponsored study

The Introduction of Brazil's Inclusive IPS Called Pix Is Contributing to Inclusivity

About 72 million Brazilians began using digital payments for the first time after the launch of Pix.

Usability of Pix is expanding beyond the P2P use case as end users are increasingly relying on the Inclusive IPS to pay for goods and services. As of June 2023, P2M use case accounts of 29% of transactions.

Average Pix transaction value is decreasing, indicating usage of Pix for everyday purchases.

We consider Pix a public good that has been set up to positively impact the economy, financial system, and people's lives. Digitizing of payments is very important for our country. We are pleased Pix is processing a high volume of transactions and that people are realizing its benefits for many use cases.

Carlos Brandt

Head of Management and Operations for Pix
Central Bank of Brazil

Impact of Inclusive IPS Fraud

Experiences of fraud can be financially and emotionally costly. Low financial and digital literacy among low-income and women end users makes them more vulnerable to fraud negatively affect their trust in and reliance on Inclusive IPSs.

Distrust of the financial system was cited by 23% of unbanked adults as the reason for not having an account.

Findex 2022

Women tend to have a higher lack of trust in financial services and providers.

Global Banking Alliance for Women, USAID

In India, three in 10 respondents stopped using DFS after a fraud event.

BMGF-sponsored study

BMGF-sponsored qualitative and quantitative studies in Ghana, Uganda, and India uncovered the following impacts to end users as a result of instant payments fraud:

Across all three markets, **respondents described an intense emotional toll after falling victim to fraud**, with feelings of shame, anger, and depression common. Indians, more than in the other two study markets, reported blaming themselves for falling victim to fraud in DFS.

Respondents said impact to livelihoods can be severe when losses were high. Respondents in Uganda and Ghana reported missing payments for school fees, delaying medical treatment and business expansion, and cutting back on monthly household expenditure including food expense. In India, where losses were milder, respondents reported minor cutbacks to monthly expenditures.

After a fraud event, **victims said they have little recourse beyond learning how to avoid falling victim a second time.** For respondents who chose to report a fraud event to the DFS provider on whose network the fraud occurred, efforts did not result in funds recovery and sometimes resulted in victim shaming.

I felt very, very bad because [when] I got frauded, that was my last money. What am I going to use? So, I was very frustrated.

Woman End User, Koforidua

My own [fraud loss] affected my job. The fraudsters, the money that they took from my account, I was going to use it to buy the materials for my customers for dresses and things and they defrauded me. So I didn't even open the store for almost a month.

Woman End User, Takoradi

Types of Fraud in Inclusive IPSs

Fraud is an intentional act, misstatement, or omission designed to deceive others, resulting in the victim suffering a loss or the perpetrator achieving a gain.

At the highest level, Inclusive IPS push payment fraud is often categorized by regulators and private sector players as authorized or unauthorized, referring to the party that initiated the payment. These are simplified categories and the tactics or vectors used by fraudsters to perpetrate these frauds come in many flavors.

Authorized Push Payment Fraud

Payment is initiated by the legitimate account owner. The end user may have been manipulated to send the payment that she believed was legitimate. The end user may have also knowingly sent a fraudulent payment.

Unauthorized Push Payment Fraud

Payment is initiated by an unauthorized end user who may have taken over the account of a legitimate end user or otherwise obtained and used the legitimate account owner's information to send a fraudulent payment.

Fraudsters Invoke a Multitude of Tactics to Conduct Push Payment Fraud

Obtaining confidential end user data through singular or multiple means enables fraudsters to perpetrate push payment fraud.

For example, a fraudster may directly obtain account login information from a **data breach** at a DFSP. This may provide them with sufficient information to do an **account takeover** and initiate an unauthorized payment from the end user's account.

The fraudster may also use the breached information to target end users for scams. **Social engineering** is a common tactic fraudsters use to scam end users to authorize and initiate payments.

Scams come in many forms. A couple of typical examples include:

- A scam may involve a fraudster pretending to be an entity that the end user knows and trusts, such as their bank or utility company, asking them to initiate an urgent payment.
- In "mistakenly sent you money" scams, the scammer sends an SMS purporting to come from a DFS provider informing the victim that they have received funds. This is followed up by a phone call in which the scammer tells the victim that the funds were sent by mistake and requests that the funds be transferred back to the scammer's account.
- The impact of these scams is noteworthy. Globally, an estimated 293M scam reports were filed and $55.3B lost in scams in 2021[1].

The fraudster may use a combination of these tactics to conduct **SIM swap**. In a SIM swap, a fraudster pretends to be the end user and is able to transfer an end user's phone number to the fraudster's device. The fraudster can then create new account login information without the end users' knowledge and take over their account.

There are many examples of push payment fraud. Fraudster tactics are continually evolving and becoming more sophisticated. A consistent classification and understanding of the details of fraud typologies are essential to identifying the controls required to mitigate each.

1: GASA – The Global State of Scams Report - 2022

What Is Fraud Risk Mitigation?

Without a concerted ecosystem commitment to fraud risk mitigation, the persistence of fraud may threaten to overshadow the benefits of Inclusive IPSs to low-income and women end users.

Fraud risk mitigation is the application of controls by payment ecosystem stakeholders to protect the integrity of the ecosystem from reputational and financial harm. "Fraud risk mitigation" and "fraud risk management" are often used interchangeably.

Certain controls are cross-cutting, while others are applied (and most beneficial) at specific stages of a payment. Strong fraud risk mitigation requires the application of all categories of controls.

Cross-Cutting

Ecosystem actions and controls that strengthen risk mitigation along multiple stages of the payment journey

Before Payment	During Payment	After Payment
Controls applied before the end user submits a payment.	Controls applied once a payment is submitted by the end user.	Controls applied after the payment is processed.

Value of Friction

The implementation of fraud mitigating controls may introduce some frictions to the payment journey experienced by end users. The benefit of a safer instant payment system that end users can trust more than offsets these frictions.

Fraud poses a tangible risk to the financial livelihoods of low-income DFS users, as we see end users missing, delaying, or cutting back on key household expenditures following a fraud event. Effective fraud mitigation is necessary and achievable to ensure the continued growth and usability of inclusive, interoperable payments systems.

Matt Bohan

Senior Program Officer, Payments Infrastructure, Inclusive Financial Systems
Global Growth and Opportunity, Gates Foundation

Strength in Collaboration

There is no single solution, action, or entity that can alone eliminate the risk of fraud in Inclusive IPSs. Each entity can support parallel and joint fraud mitigation efforts that result in more effective outcomes for the ecosystem.

Inclusive IPSs

The connective tissue of the payments value chain. Inclusive IPSs can support fraud mitigation through:

- Scheme rules
- Fraud mitigation tools (for themselves and for the ecosystem)
- Governance structures, including forums for collaboration

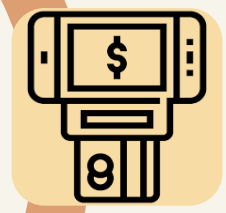
DFSPs

Account providers to end users and participants in Inclusive IPSs. DFSPs are best positioned to implement fraud risk controls, including:

- Customer onboarding and due diligence measures
- End user fraud education and tools
- Business and technical practices for transaction risk management
- Receiver confirmation tools
- Proper recourse and liability mechanisms

Fraud mitigation actions by one stakeholder often complement, enhance, and inform actions by other stakeholders.

Intentional collaboration between ecosystem stakeholders improves fraud mitigation for all.



Regulators

Provide the foundational tone and platforms for fraud mitigation through:

- Standards, guidelines, and requirements that pertain to Inclusive IPSs, DFSPs, and other industry players
- Forums for ecosystem collaboration

Payment Service Providers

Other entities that participate in the payments value chain, e.g., fintechs, agents, third-party service or technology providers. They can contribute to fraud mitigation through:

- Appropriate fraud mitigation approaches
- Fraud mitigation technologies and solutions

Others

Various other entities play important roles in the ecosystem, including:

- Law enforcement entities ensure laws and regulations are followed
- Industry bodies contribute to forums for collaboration between ecosystem parties
- Consumer groups capture and advocate for end users

End Users

Payment senders and receivers. When properly buttressed by the ecosystem with necessary tools, end users can contribute to fraud mitigation through:

- Payment scam identification
- Authentication tools use

THE LEVEL ONE PROJECT

Section 2

Core Tenets of Fraud Mitigation

2

End Users Are Not Liable for Fraudulent Payments

Tenet 1: Liability

End users are not liable for confirmed fraudulent payments.

Context

Motivations and incentives to mitigate fraud risk must be aligned

The experience of fraud and any associated loss of funds can have a severely negative and immediate impact on low-income and women end users, including the inability to have sufficient funds for basic daily needs. The occurrence of fraud may also lead to a loss of trust in DFSPs (the participants in Inclusive IPSs) and use of their services. Potential loss of customers and revenue should provide the impetus for DFSPs to mitigate fraud risk.

However, this may not provide sufficient motivation or ability for a DFSP to address the risk alone.

Regulations provide key guidance

Clarity in laws and regulations (reinforced by scheme rules) that the end user is not to be held responsible for financial loss due to confirmed fraudulent payments (in cases where the end user is not complicit in the fraud) is an important starting point in **aligning motivations and incentives** toward improved fraud mitigation.

In many markets, regulations are in place to protect the end user from the harmful impact of fraud. These regulations typically specify that end users are not financially liable for fraudulent payments they did not authorize. In light of rising authorized push payment (APP) fraud, regulators are increasingly evaluating or implementing policies that entitle end users to refunds in cases of APP fraud.

The details of the regulations vary. Financial liability for fraudulent payments may be allocated to the DFSP (sending, receiving, or both) and/or other entities involved in the payment value chain (and whose controls failed to prevent fraud). Standards on end user fraud reporting also may differ (e.g., how, to whom, and submission deadlines for disputes) and the details of funds refunds (e.g., how quickly the funds must be returned to the end user).

Minimum guidance to mitigate fraud risk and refunds

Guidance offered to decrease fraud risk, and therefore fraud liability, may change over time should be influenced Guidance will typically include DFSPs applying know-your-customer (KYC) risk-based controls, end user authentication, tools that screen payments for fraud, investigation processes to determine whether fraud has occurred (including an independent body to be a final arbiter), simple and accessible tools for end users to report fraud, and mechanisms to return end user funds in a timely manner.

Role of the Inclusive IPS

Inclusive IPSs play an important role in guiding and supporting DFSPs

As participants in Inclusive IPSs, **DFSPs play the primary role in mitigating fraud risk** for their customers and the broader Inclusive IPS ecosystem. However, the Inclusive IPSs should support them by being clear and detailed in their rules on strong risk management (Tenet 2), providing tools for DFSPs to use (Tenet 3), and sharing data and information to enable the tools and operational controls to be most effective (Tenet 4).

Regulators have an important responsibility to provide a robust regulatory and supervisory foundation on fraud mitigation. Their guidance gives direction to financial institutions in stopping scams and fraud from happening and in better protecting and providing a remedy for people if they do fall victim.

Innovation in regulations will need to keep pace with evolution in fraudsters' tactics.

Scheme Rules Guide DFSPs

Tenet 2: Rules

The Inclusive IPS guides DFSPs in managing fraud risk through their scheme rules.

Context

Strong risk management requires guidance

Regulatory standards on DFSP fraud risk management are commonplace and are often captured in central bank or government directives, consumer protection guidelines, licensing requirements for DFSPs, and supervisory guidance. The standards may relay principles or share precise and prescriptive requirements. Regardless, they provide a critical basis for defining DFSPs' fraud mitigation responsibilities and often have a broader objective of ensuring the overall safety and soundness of the financial system.

For regulatory guidance to be effective, it requires consistent enforcement that includes penalties for noncompliance.

Role of the Inclusive IPS

Scheme rules may directly incorporate existing regulatory standards. ***Importantly, they should strengthen fraud mitigation by mandating DFSPs to implement specific actions and practices in order to participate in the Inclusive IPS.***

Regulatory guidelines are helpful in highlighting expectations for strong fraud management, but they do not usually define DFSP requirements for participating in specific payments system (exceptions exist).

The Inclusive IPS' scheme rules play a key role in providing that specific guidance and raising the bar on risk management. Scheme rules need to ensure that all DFSPs participating in the system adhere to a set of standards that are designed to keep the Inclusive IPS safe and sound by preventing fraud from occurring in the first place, and to minimize its impact.

Strong KYC controls are critical in aligning the level of risk a customer brings to controls to minimize potential impact of fraud if it occurs. **End user authentication** methods, education, and confirmation of payee provide controls before a payment is initiated. Once a payment is in flight, **transaction screening** mechanisms, whether at the DFSP or Inclusive IPS level (or both), provide a tool for flagging and potentially preventing fraudulent payments.

Even with these controls in place, some fraud will occur. To mitigate the negative impact on end users, accessible and effective mechanisms need to be in place for end users to lodge **fraud complaints and request return of funds**. DFSPs need to have robust processes to investigate those complaints, determine whether fraud has occurred, and in cases of confirmed fraud, to follow a process to return funds to the end user as quickly as possible.

Importance of collaboration

As fraudster tactics and fraud risks evolve, regulations, laws, and scheme rules will need to follow. The Inclusive IPS is well positioned to provide leadership or actively participate in collaborative efforts to evolve rules and standards. A collaborative approach to evolving these will drive alignment, ensure clarity, increase comprehensiveness, and ultimately reduce fraud risk for the entire ecosystem.

Scheme rules define a set of requirements, standards and practices necessary for the functioning of an IPS and for participating in a system.

Scheme rules are often supplemented by **operating procedures**, which provide a more detailed set of technical and operational requirements for participating in the scheme and connecting to the IPS.

Inclusive IPSs Provide Tools

Tenet 3: Tools

The Inclusive IPS provides fraud mitigation tools and share in the investment.

Context

Fraud mitigation requires multiple tools

The Level One Project supports an open, competitive Inclusive IPS ecosystem where a variety of licensed financial institutions can serve as DFSPs. These DFSPs likely vary in their business models, operational capacity, and fraud risk management resources.

Moreover, managing fraud in a 24x7x365 environment is challenging and operationally demanding. It may also be costly and require new resources.

To comply with regulations and adhere to scheme rules, DFSPs rely on a myriad of fraud mitigation tools.

Fraud mitigation should not be a competitive advantage

A **shared investment in fraud mitigation tools** can be particularly helpful in preventing fraud occurrences across the ecosystem. Investment in tools by the Inclusive IPS can help reduce the cost of fraud risk mitigation for individual DFSPs and the ecosystem.

Role of the Inclusive IPS

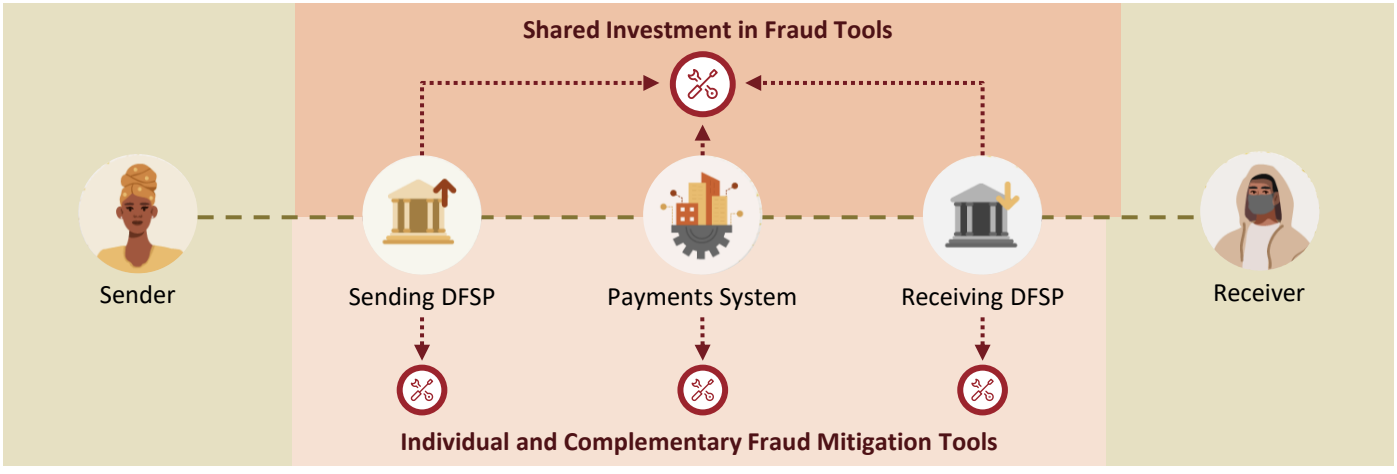
Inclusive IPSs should enable DFSPs in achieving a higher standard of fraud mitigation by providing fraud mitigation tools for DFSP use and implementing tools at the Inclusive IPS platform level

Real-time transaction screening or monitoring systems that are designed to detect unusual payment patterns and to stop suspicious transactions from being processed are a particularly valuable component of fraud risk mitigation.

The tools implemented by the Inclusive IPS itself can complement DFSP efforts. For example, the Inclusive IPS can also screen transactions for bad actors, incorporating information they capture across different participants. The Inclusive IPS can also develop and provide other valuable fraud mitigation solutions, such as a catalog of fraud typologies, confirmation of payee, and a safe payment-addressing approach.

An arrangement where all parties operate **solutions that are complementary** is most effective as fraudsters understandably work across DFSPs. These solutions vary in scope and may be implemented by the Inclusive IPS and/or by the individual DFSP.

Inclusive IPSs should also provide tools to DFSPs to help simplify the complaint process for end users and support the resolution process for DFSPs. These may range from one click fraud reporting, shared fraud notifications between DFSPs, white-labeled wallet with anti-fraud notifications, AI-enabled chatbots, fraud investigation coordination tools and services, and others.



Data as Enabler of Risk Mitigation

Tenet 4: Data

The Inclusive IPS establishes fraud data and information-sharing guidelines and mechanisms.

Context

Data is essential to understanding and reacting to fraud

The ability to mitigate fraud risk is dependent on ecosystem stakeholders having a clear understanding of the types of frauds that are occurring, a shared language to describe them, and an awareness of the vectors and methods through which fraud is perpetrated. The ability to appropriately capture, analyze, and responsibly share this data is essential to successful fraud risk management. For example, regulators often require DFSPs to submit fraud data for analysis and to better understand fraud trends and use these to inform standards and policies.

Role of the Inclusive IPS

Inclusive IPSs provide data-sharing guidelines, methods, and environments to affect fraud risk mitigation

The effectiveness of tools implemented by DFSPs and Inclusive IPSs is highly dependent on the availability and quality of the inputs (data and information).

Appropriate data and information sharing increases fraud mitigation efficacy.

DFSPs should have mechanisms in place to capture and analyze transaction data to identify patterns that may indicate a transaction is suspicious; a transaction may be assigned a risk score to indicate the likelihood that it may be suspicious.

Inclusive IPSs can also benefit from receiving DFSP data. For example, access to DFSPs' ON- and OFF-US transaction data, including which transactions are confirmed by DFSPs to be fraudulent, is critical for the Inclusive IPS to evolve effective transaction monitoring tools since the data informs what constitutes a typical versus unusual payment pattern.

Similarly, DFSPs can benefit from Inclusive IPS data. Expanding and complementing DFSPs' activities, Inclusive IPSs should have rules and procedures that allow them to identify suspicious payment patterns and notify DFSPs accordingly. Similarly, they may identify bad actors with goal of preventing a bad actor from holding accounts at multiple DFSPs.

Balance data and information sharing with necessary security and privacy measures

Data security and privacy guidelines are critical to ensure data is protected and used responsibly. More specifically, data security controls need to be in place to ensure that all data is collected, stored, and transmitted in a way that prevents access and use by unauthorized parties. Data privacy controls ensure that consumer data is collected in a transparent manner and used with consumers' express consent.

Regulators play a vital role in defining consumer and data protection guidelines that the scheme rules should echo and potentially, build upon. **Together with law enforcement entities, they also must ensure that the laws and regulations are followed**, that fraudsters face repercussions, and that end users and their data are protected.

Data sharing is a powerful tool in fraud mitigation. But in the wrong hands, consumer data can also be used to commit fraud and undermine consumers' trust in digital financial services. As a result, fraud data collection and sharing approaches must be supported with strong consumer and data protection regulations.

Anna Wallace
Senior Program Officer, Consumer Protection, Inclusive Financial Systems
Global Growth and Opportunity, Gates Foundation

THE LEVEL ONE PROJECT

Section 3

Inclusive IPS Fraud Mitigation Approaches

3

Spotlight on Brazil's Pix

Brazil's Pix is among the newest and most successful Inclusive IPSs. As the Pix rules authority and operator, the Central Bank of Brazil has taken a very active approach toward increasing adoption.

2020	Central Bank of Brazil	800+	24B
Launch Year	Rules Authority	*Banks and Non-Banks* Participating DFSPs	2022 Transaction Volume

In its regulatory and rules authority capacity the Central Bank of Brazil is responding to incidences of fraud in Pix by increasing requirements on participating DFSPs and supporting DFSP risk management efforts by providing shared tools.

What's Notable Related to Fraud Mitigation?

Pix rules specify numerous DFSP requirements, including those on tools for end user authentication and verification of security and validity of payment requests. *The controls required by the scheme at the pre-payment and payment stages of the journey contribute to raising the bar on DFSPs' risk management.*

DFSPs are also required to report suspicious fraud transactions to a centralized database maintained by the Pix scheme. Consultation of this database by DFSPs was initially optional and is now required. DFSPs must use the information either to decide whether to authorize transactions, reject them, or hold back for further analysis. If held, DFSPs can take 30 minutes during daytime and 60 minutes at night to conduct additional analysis. They may also use the information in the database for other internal processes, such as account opening.

Requirement to report fraudulent payments is designed to support all DFSPs in their transaction screening processes.

Complaint and Resolution Mechanisms: Pix rules provide a Special Mechanism for Return to enable the return of funds in cases of suspected fraud or operational failure in the system technology.

The Pix-provided tool enables parties to more easily initiate fraud complaints.

If unable to reach resolution, the parties can initiate a formal dispute to the Central Bank of Brazil. The Central Bank standardizes the procedure and deadlines for complaint resolution, giving the user more clarity about the process. As soon as the user makes a complaint to his or her DFSP, the other DFSP in the transaction receives the information and blocks the credited funds.

Alias addressing: Pix maintains a directory that supports multiple forms of aliases, including a randomly generated number composed of 32 characters.

The use of a randomly generated number helps protect end user privacy by avoiding the use of personal identifiable information.

*Example of a DFSP receipt for a payment using a random alias**

**Source of image:* Pix

Spotlight on India's UPI

India's Unified Payments Interface (UPI) scheme was introduced on top of Immediate Payment Service (IMPS) to increase adoption by adding features such as payment initiation through third-party service providers and alias addressing. UPI is considered a public good and has mandated no charge for person-to-person transfers.

2016	National Payments Corp. of India (NPCI)*	390+	74B
Launch Year	Rules Authority	*Banks and Non-Banks* Participating DFSPs	2022 Transaction Volume

UPI scheme rules and India's regulations set detailed and prescriptive requirements for DFSPs on various elements of fraud risk management, including end user authentication, fraudulent transaction reporting, and dispute mechanisms.

What's Notable Related to Fraud Mitigation?

UPI rules include prescriptive requirements with respect to end user authentication and identification. For example, for request-to-pay messages, DFSP must decline transactions where the receiver identity is masked. To prevent SIM swap fraud, rules prescribe strict guidelines around end user changes in mobile numbers. Lastly, rules articulate additional DFSP fraud control recommendations, like velocity checks.

The controls required by the scheme contribute to raising the bar on DFSPs' risk management.

India, through both UPI scheme rules and general consumer protection regulations, requires DFSPs to provide transaction notifications and multiple complaints channels that enable the reporting of suspected fraudulent transactions. For disputes of reported fraudulent transactions, UPI scheme rules provide detailed steps to determine liability with an NPCI panel to address unresolved disputes between DFSPs. An Ombudsman appellate authority at the Reserve Bank of India (RBI) provides another resolution body in case disputes require it.

Complaint and dispute mechanisms provide necessary fraud corrective measures.

**Nonprofit umbrella organization overseen by the Reserve Bank of India*

Spotlight on Ghana's GIP

Ghana's GhIPSS Instant Pay (GIP) is an interbank Inclusive IPS; it forms the foundation for the "financial inclusion triangle," which enables interoperability between GIP, MMI (mobile money scheme), and e-zwich (stored value bank card scheme). Volumes have increased notably since 2019.

GhIPSS	**2015**	**GhIPSS***	**50+**	**76M**
	Launch Year	Rules Authority	*Banks and Non-Banks* Participating DFSPs	2022 Transaction Volume

Bank of Ghana (BOG) has issued several extensive directives on fraud risk management, consumer protection, and fraud reporting that DFSPs licensed by BOG. BOG is taking a proactive approach to updating the regulations as fraud trends and risks evolve.

What's Notable Related to Fraud Mitigation?

The extensive directives issued by BOG apply to the DFSPs that participate in GIP. Notable regulations include those that define risk management approaches related to anti-money laundering (AML), combating the financing of terrorism (CFT), and customer due diligence (CDD) as well as provide guidance on consumer recourse mechanisms. *Scheme rules reinforce these regulations to raise ecosystem-wide fraud mitigation.*

BOG requires banking institutions, specialized deposit-taking institutions (SDIs) and electronic money issuers (EMIs) to report attempted and successful fraud incidents and publishes this data in an annual report. Along with the data, the report is used to provide specific recommendations to these institutions on strengthening their risk management activities. *Fraudulent payment reporting requirements strengthen future actions.*

The annual publication of the report by BOG is an example of a tool used to track fraud trends. While not all institutions are yet providing their data, the report is a meaningful starting point to encourage reporting.

Spotlight on the US' FedNow

The FedNow Service is the newest instant payments system, launched in the United States in July 2023. The FedNow Service is operated by the Federal Reserve and will be available to all US financial institutions (10,000+).

FedNow	2023	Federal Reserve	100+	Not Yet Available
	Launch Year	Rules Authority	*Banks and US Dept. of Treasury* Participating DFSPs	Transaction Volume

The FedNow Service launched with shared tools at the scheme level to enable financial institutions of all sizes to raise the bar on fraud risk management, with a focus on fraud reporting and transaction screening.

The Federal Reserve has signaled that these tools will be enhanced and additional tools will be added over time.

What's Notable Related to Fraud Mitigation?

The scheme rules require a participating DFSP to report to the FedNow Service and to the other DFSP if after investigation, it believes a transaction was fraudulent. The FedNow Service provides a non-value message to DFSPs to support the reporting. The rules specify that participating DFSPs may only use this information for purpose of remediating, investigating, and preventing fraudulent activity.

Fraudulent payment reporting does not stop or reject the transaction as it occurs and instead, it is designed to enable DFSPs and the scheme to over time gain more insights into fraud patterns and enhance transaction screening.

The FedNow Service also supports DFSPs by providing controls to supplement their risk mitigation practices. While not exclusively intended to prevent fraudulent transactions, DFSPs have the option to turn on a functionality in the FedNow that screens transfers against a Negative List (provided by the DFSPs, the list contains the combination of a DFSP identifier and end user account number); a transfer that matches the combination on the list will be rejected.

The screening capabilities tool provided at the scheme level allow DFSPs to prevent potentially fraudulent transactions.

Spotlight on UK's FPS

The UK Faster Payments Service (FPS) was among the earliest IPS to launch, serving as inspiration for these systems globally. Banks have access to FPS directly or indirectly. Other payment service providers may also access FPS, depending on type of connection.

2008	Pay.uk	35+	4B
Launch Year	Rules Authority	Banks and Non-Banks Participating DFSPs	2022 Transaction Volume

Over the last few years, the UK has seen an increase in authorized push payment fraud that is negatively affecting end user trust in the system. In response, the regulators and scheme rules authorities are responding by advocating for greater clarity in financial liability allocation, more specific DFSP risk management requirements, and shared tools, including improved fraud reporting mechanisms.

What's Notable Related to Fraud Mitigation?

The Payments Systems Regulator and pay.uk are collaborating to develop rules that will make FPS participants liable for refunding end users who sent funds as a result of APP fraud.

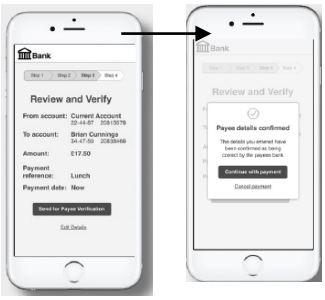
Allocating financial liability for confirmed fraudulent events to DFSPs will reinforce importance of strong risk management by DFSPs.

The scheme rules already emphasize that DFSPs have primary responsibility for fraud mitigation and undertake *suitable fraud checks in line with their own policies* and refer DFSPs to follow *prevailing legislative requirements regarding AML and the KYC process.*

Specific requirements provide important guidance for DFSPs on effective risk management.

The *confirmation of payee* functionality provided to DFSPs enables a sender to validate if the name on the receiver account matches the name and account details of the person or business they intend to send money to before initiating the transfer.

Confirmation of payee is one tool that may enable end users in preventing fraudulent payments.



Illustrative flow of positive confirmation of payee

Finally, in its fraud strategy the UK government has committed to a comprehensive set of actions that includes development of additional fraud mitigation tools, improved fraud reporting mechanisms for end users, an appointment of an Anti-Fraud Champion to ensure collaboration of fraud initiatives across public and private sectors, and commitment to publish new regular data on patterns of fraud.

These efforts are intended to contribute to further mitigate fraud and build end user trust in the payments system.

Source of image: https://www.wearepay.uk/wp-content/uploads/2019/10/Confirmation-of-Payee-brochure.pdf

THE LEVEL ONE PROJECT

Section 4

Fraud Mitigation Design Guidance

4

Design Guidance: Putting Fraud Mitigation into Practice

Core tenets of fraud mitigation come to life through of practical design guidance.

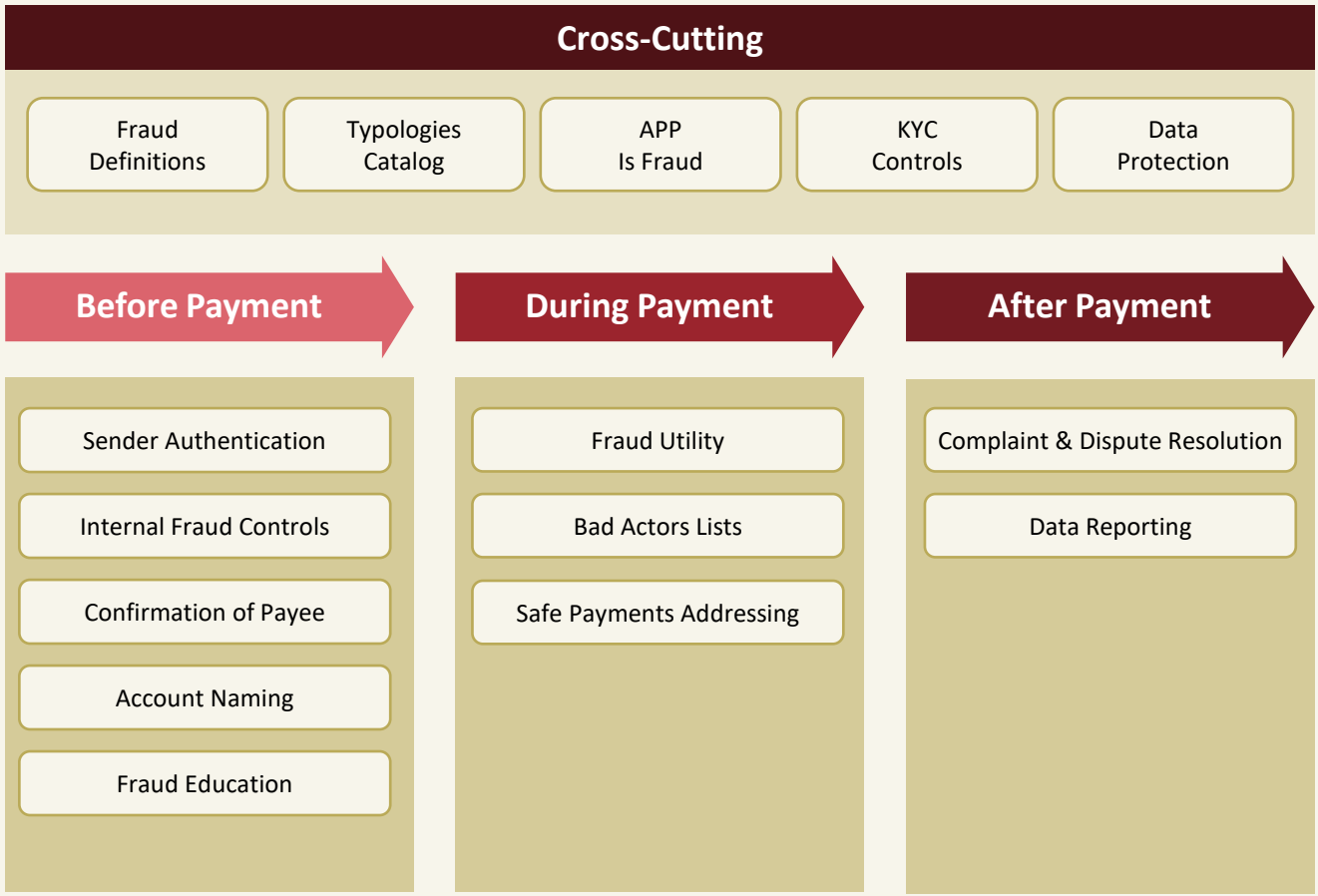
No single best practice will sufficiently mitigate the risk of fraud.

The application of a set of design guidance, which aims to prevent, detect, and respond to fraud, will provide the best chance of minimizing the occurrence and impact of fraudulent payments.

The choice of which guidance to implement will be somewhat context-specific. The guidance featured in this section is considered high-impact and comprehensive but are not exhaustive.

Just as Inclusive IPSs transform in response to end users' needs, and as fraudsters evolve their tactics to be more successful in perpetrating fraud, this guidance will need to evolve over time to ensure it remains relevant and supportive of fraud mitigation.

The following pages describe design guidance and indicate which tenets each supports. A summary of the link between core tenets and guidance can be found on page 38.



Cross-Cutting Guidance (1 of 2)

Guidance 1: Fraud Definitions

Liability | Tools | Data

The Inclusive IPS provides a framework for defining fraud types.

A common global framework for talking about the push payments fraud does not yet exist. Clarity and consistency in defining fraud is needed for effective collection of fraud data, analysis of fraud patterns and trends, assigning of liabilities, and as a result, stronger risk mitigation.

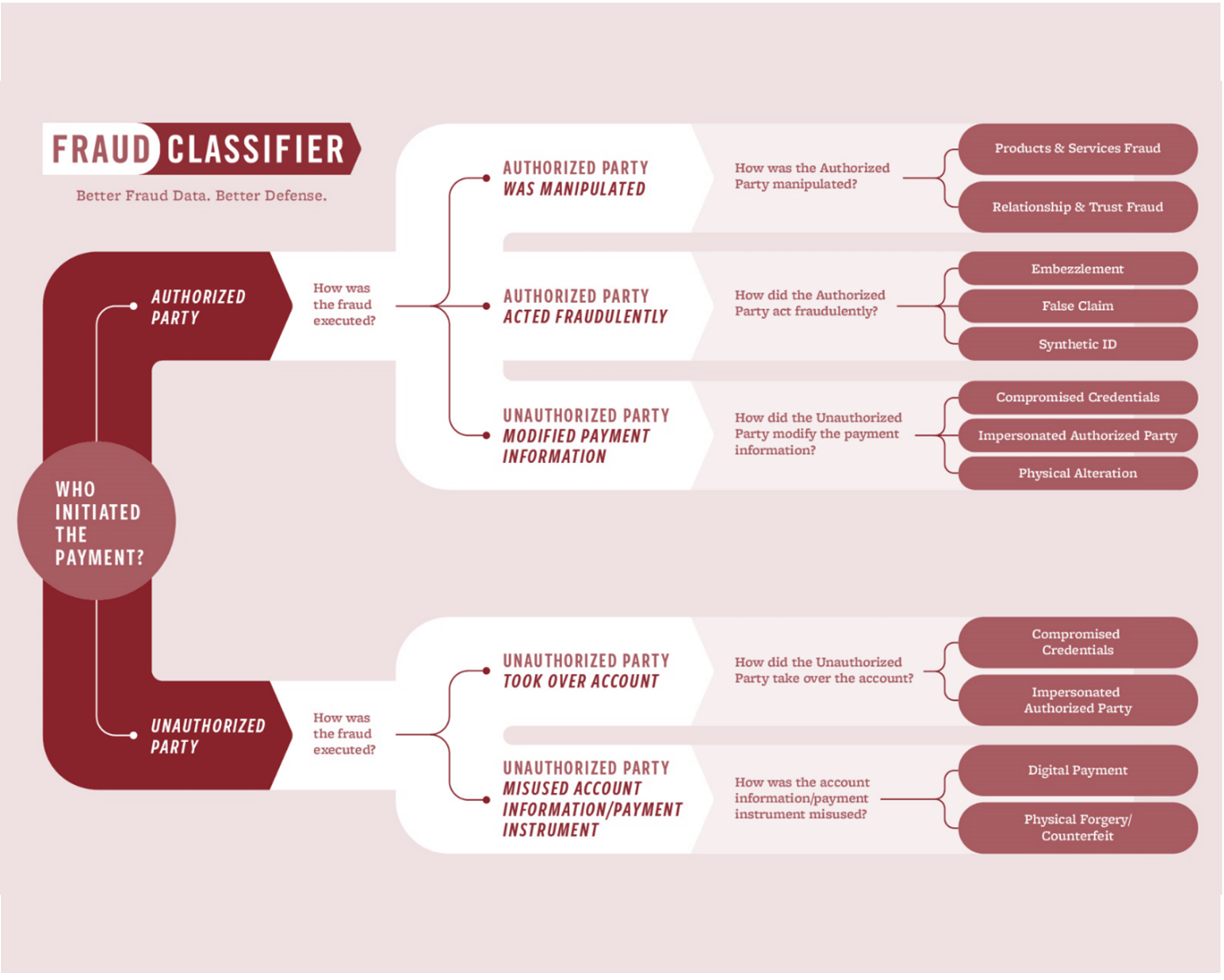
Definitions and classification frameworks are often developed through collaboration. Regulators often serve as the ecosystem conveners. Inclusive IPSs may also lead these or support these efforts.

Inclusive IPSs' scheme rules can mirror or reference existing definitions and fraud type frameworks; in cases where they do not exist, scheme rules should provide them.

Example:

The FraudClassifier model (see below), which was developed by the payments industry under the leadership of the US Federal Reserve to provide a basic fraud classification.

At the highest level, it categorizes fraud based on who initiated the payment (an authorized or unauthorized party) and how it was executed.



Source: https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/fraudclassifier-model/

Cross-Cutting Guidance (2 of 2)

Guidance 2: Typologies Catalog

Tools | Data

The Inclusive IPS leads or participates in collaborative efforts to define and evolve a fraud typologies catalog. The catalog is made available to DFSPs for use in transaction screening.

A common language for talking about fraud is essential, but alone not sufficient. Fraudsters perpetrate fraud in a myriad of ways, which include sophisticated tactics and multistep approaches along a payment journey. A close understanding of the details of fraud typologies will allow ecosystem stakeholders to identify and put in place appropriate controls. Specifically, typologies can be reflected in transaction monitoring systems as a set of rules used to screen for potential fraudulent payments.

Creating an accurate and comprehensive fraud typologies catalog will require collaboration. Fortunately, in many markets DFSPs, Inclusive IPSs, regulators, and other experts within the ecosystem commonly meet to align on best practices.

The most useful typology will provide a framework for cataloguing and reflect true fraud vectors, as they evolve.

Guidance 3: APP Is Fraud

Liability

The Inclusive IPS considers payments that have been authorized as a result of social engineering, in which the legitimate end user is not complicit, to be fraudulent.

Financial liability rules should scope fraud to include the most common and concerning fraud types. Specifically, payments that are confirmed to have been authorized as a result of social engineering, in which the authorizing end user is not complicit, should be considered fraudulent.

The fraud definitions framework provides an important base for successful alignment with this guidance.

Example: This is a topic of active current debate by regulators and Inclusive IPS. UK regulators are pushing for regulations to require payment service providers to reimburse funds lost to end users due to APP fraud. The European Commission is evaluating adding APP fraud to its liability and refund rules. In the US, Inclusive IPSs (most notably, Zelle) are increasingly under pressure to incorporate more clarity in their rules on fraud liability.

Guidance 4: KYC Controls

Rules | Tools | Data

The Inclusive IPS requires DFSPs to apply controls appropriate for each KYC tier and customer risk profile.

DFSPs are naturally incentivized to appropriately align controls to each customer risk profile and KYC tier to manage their risk exposure.

Controls may pause services. For example, DFSPs may require that a new customer cannot withdraw funds deposited into their account for a certain (short) time period. This type of control can help DFSPs to identify if the new account was opened in order to perpetrate fraud.

Controls may limit services. Limits on the value or volume of transactions that a customer is permitted to conduct can also be beneficial. While the application of limits is not strictly a fraud prevention tool, applying these limits may minimize the financial impact of fraud events. Inclusive IPSs commonly elect to have high or no transaction value limits at the scheme level in order to enable a variety of use cases. However, they should not prohibit (and may encourage) DFSPs from setting lower limits for individual end user accounts.

Guidance 5: Data Protection

Rules | Data

The Inclusive IPS provides guidelines for confirmed fraud reporting and safe use of data to protect end user privacy and DFSP data confidentiality.

While data is a key enabler of fraud mitigation, data sharing, storage, and use may introduce other risks if it is not properly safeguarded. Consumer protection considerations should be incorporated into the design of all risk mitigation controls to ensure that end user data is protected.

Payment messages often capture and transmit rich data elements including sometimes personally identifiable information on end users. Sharing of that data, even for fraud mitigation, requires controls to protect end user privacy and DFSP data confidentiality. Inclusive IPSs can play an enabling role by establishing clear guidelines for participants on safe use of data, incorporating and building on available regulatory guidelines.

Guidelines may include requiring end user consent on use of certain data elements, limiting access to the data, and use of the data for fraud mitigation purposes only.

Before-Payment Guidance (1 of 2)

Guidance 6: Sender Authentication

Rules

The Inclusive IPS requires DFSPs to utilize multiple tools and controls to authenticate end users.

Sender authentication tools verify that the sender is who they claim to be. Different tools may support authentication.

Multifactor authentication is a common approach that requires the end user to verify their identity with a combination of something they have (e.g., a mobile phone), something they are (e.g., their fingerprint or iris scan), or something they know (e.g., a PIN or password). Use of multiple methods to authenticate senders will more effectively prevent fraud.

Not all tools will be applicable to each end user, context, or use case. For example, an end user that relies on a feature phone cannot biometrically authenticate but will be able to verify their identity with their phone number and PIN. A DFSP may additionally apply device identification methods, such as matching the user's identity to physical device identifiers.

Example: India's UPI system provides a set of prescriptive end user authentication requirements.

Guidance 7: Confirmation of Payee

Rules Tools

The Inclusive IPS enables a confirmation of payee (CoP) service that allows end users to verify the name of the receiver prior to initiating a payment.

A confirmation of payee service may prevent authorized push payment fraud where a sender is scammed to sending a payment to a fraudster's account. (It can also prevent funds being sent to an unintended party due to errors in keying their alias or account number.) The application of CoP allows the end user to see the name (e.g., first and last name of consumer or name of business) associated with a receiver's account number or alias prior to sending a payment. An unexpected name may signal to the end user that the receiver is not the intended party, leading them to cancel the payment.

CoP introduces an additional end user touchpoint into the payment initiation flow. When well designed and implemented, CoP can contribute to preventing fraudulent payments, making the additional step a worthwhile trade-off.

Example: UK's Faster Payments has enabled confirmation of payee. Pix also mandates that payee identification be displayed in the payer's screen at payment initiation.

Guidance 8: Internal Fraud

Rules

The Inclusive IPS requires DFSPs to implement controls designed to prevent a DFSP employee from perpetrating fraudulent payments.

Fraud may be perpetrated by DFSP employees. The application of internal operational controls contributes to preventing this type of fraud. At a minimum, these include controls that strictly restrict access rights to critical transaction systems, dual controls that require more than one individual to initiate or review transactions, and separation of duties that prevent a single individual from playing too many important roles in a process.

Guidance 9: Account Naming

Rules

The Inclusive IPS requires DFSPs to utilize clear and descriptive account-naming conventions.

For tools such as confirmation of payee to work effectively, DFSPs' customer onboarding processes need to ensure that internal names assigned to consumer and business accounts provide a clear indication of who the customer is. For example, a company account could be identified by the company name and a consumer account by the first and last name of the account holder or other preferred identifier (e.g., a nickname or initial for first name). As part of the confirmation of payee, the name of the payee should be displayed to the payer once they enter the alias for the receiver's account.

Clear account naming is relevant across use cases. For example, in a QR-enabled merchant payment, fraud may be prevented by displaying the merchant name to the payer before they confirm the transaction.

Before-Payment Guidance (2 of 2)

Guidance 10: Education

Rules Tools

The Inclusive IPS requires DFSPs to educate end users, employees, and partners on fraudster tactics and mitigation practices on an ongoing basis and at payment initiation using proven approaches.

End users contribute to mitigating fraud by staying alert to fraudster tactics and when possible, stopping a fraud attempt by not initiating a suspicious payment. An end user educated about fraud can be a powerful tool of fraud prevention, but it is just one tool and alone will not prevent all fraud events.

For fraud education to be effective, it needs to be multilayered, part of multiple stages of the end user payments journey, and appropriate to the local context. Use case specific education, such as educating customers to be alert to fake merchant QR codes, should also be considered. Ongoing education may be provided through a variety of channels. Education must be designed for low-income and women end users and be delivered in a relevant format and language.

The moment of payment initiation may provide a particularly good opportunity for just-in-time education. For example, when a payer initiates a payment to a merchant by scanning a QR code, they could be shown a message that reminds them to always validate that the QR code is indeed for the merchant they want to pay. An effective approach will consider the benefits of education against the trade-off of introducing too much friction.

The Inclusive IPS may play a role in supporting DFSPs in these efforts. For example, campaigns aimed at spotting fraud may be incorporated in broader Inclusive IPS advocacy or branding campaigns. The Inclusive IPS may consider developing and sharing guidelines or resources on user experience (UX) methods that have proved to be effective in capturing end users' attention.

There is no "one size fits all" approach to impactful education and achieving impactful education is challenging.[1] Inclusive IPSs and DFSPs should measure the effectiveness of their approaches and evolve them over time.

Example: Vodafone Ghana partners with the Ghana Chamber of Telecommunications to educate Ghanaians about fraud. A part of that effort was a short video skit.

The GSMA Toolkit provides skills, resources, and knowledge to digital financial services stakeholders on enabling end user digital financial literacy.

1. Callsign, White Paper on Online Fraud.

During-Payment Guidance (1 of 2)

Guidance 11: Shared Fraud Utility

Rules | Tools | Data

The Inclusive IPS provides a shared fraud utility tool to support DFSPs' transaction monitoring activities.

The Inclusive IPS should require DFSPs to monitor for suspicious transactions and be capable of preventing potentially fraudulent transactions while minimizing the impact on legitimate transactions.

The Inclusive IPS should provide a shared fraud utility tool, available for implementation by individual DFSPs, that provides these capabilities at a low cost. The shared tool could be a complement to DFSPs' transaction screening methods or be the primary DFSP screening tool depending on the specific market context.

The exact functions may vary, but at a minimum it should have the capability to score transactions based on their likelihood of being fraudulent, to be able to learn from past fraudulent transactions, and to be capable of accurate and timely reporting.

Foundational fraud utility services implemented by the Inclusive IPS are ideally offered as a core service at no or very low cost to participants.

Aspects of the shared tool may be implemented by the Inclusive IPS platform, to mitigate fraud across DFSPs.

Example: Pix allows the receiver's DFSP to put a precautionary block on funds credited to an end user account, for up to 72 hours to

What should be included in a transaction monitoring system operated by a DFSP?

Transaction monitoring systems vary in their sophistication and design; for example, they may be rules-based or utilize machine learning and/or AI. They must be capable of incorporating data on past confirmed frauds to continually update what constitutes a suspicious pattern.

Each DFSP will need to determine the right implementation for their organization, though an effective system will learn over time from confirmed fraudulent transactions and minimize the impact on legitimate transactions.

To be effective, transaction monitoring systems need to be supported by DFSPs' operational processes that include timely investigation and resolution of transactions flagged as suspicious. Consideration should be given to appropriate value thresholds to determine transactions that require investigation.

Guidance 12: Bad Actors List

Tools | Data

The Inclusive IPS provides DFSPs with the capability to submit a list of bad actors, which allows the scheme to screen transactions against the list, to reject any that trigger the list, and to share the list with DFSPs to flag accounts owned by the bad actor.

A shared bad actors list (sometimes referred to as a negative list) maintained and implemented at the Inclusive IPS platform level provides a complementary functionality to the fraud utility. The application of a negative list allows DFSPs to conclude if the sender and/or receiver are considered a bad actor. Based on the conclusion, a transaction can be rejected.

The implementation details (i.e., how negative lists are submitted to the Inclusive IPS, how new bad actors are added and others removed, and how the lists are shared between different DFSPs) may vary. The FedNow Service will have a negative list screening function that will be optional (and free) for DFSPs to use.

Example: FedNow will enable screening of transactions against the Negative List (at each DFSP's discretion).

During-Payment Guidance (2 of 2)

Guidance 13: Payments Addressing

Tools

The Inclusive IPS provides a safe payments- addressing approach.

The Inclusive IPS utilizes a directory that enables aliases for payments addressing in lieu of end user account numbers. Multiple types of aliases, such as a phone number, email, national ID number, other ID number, or a randomly generated alias may be supported.

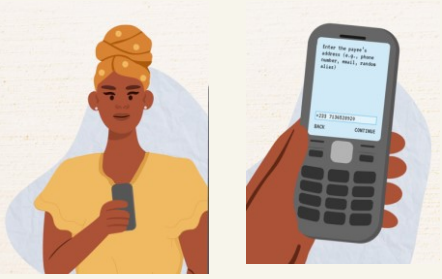
A QR code is another example of an alias, typically used to initiate merchant payments. To send a payment, a payer needs only to know the payee's alias. Masking the account information from potential fraudsters can make it more difficult for them to perpetrate fraud.

Further, providing multiple options for an alias, including options that do not include personally identifiable information, empowers end users to choose an alias most suitable for them. For example, restricting aliasing to phone numbers may make it challenging for some women to send or receive payments if they share a single phone with their husband. Women may also not feel comfortable sharing their phone number to receive a payment.

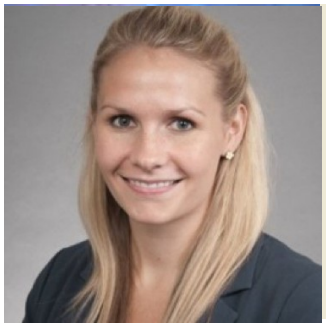
Approaches to alias and account naming (Guidance 9) should be considered together. An alias needs to be easy to remember and easy to share. An account name needs to be relatable to the receiver, and therefore the alias. In doing so, the scheme support the sender in ease of initiation transactions to the right receiver.

Example: Brazil's Pix system enables the use of a randomly generated number.

A QR code is an example of an alias used to mask an account, typically a merchant account. The end user scans the QR code using their mobile phone to initiate a payment.



An illustration of safe payments addressing as perceived by a sender.



The decision to inclusively mitigate fraud must permeate all Inclusive IPS design decisions. Safe payments addressing, whereby the payer does not need to know the payees' account number to initiate a payment, is one important example.

Cici Northup

Associate Partner
Glenbrook Partners

After-Payment Guidance

Guidance 14: Complaint and Resolution Mechanisms

Liability | Rules

The Inclusive IPS requires DFSPs to provide complaint and dispute resolution mechanisms that are clearly communicated, easy and free for end users, and appropriate to the local context.

In cases where fraud has occurred, effective complaint and dispute resolution mechanisms contribute to restoring end user trust in the system. The Inclusive IPS' relevant scheme rules should be consistent with any regulatory guidelines, which are often provided in consumer protection regulations.

Complaint mechanisms provided by DFSPs enable end users to request a return of funds due to fraudulent activity. End user rights in making complaints need to be clearly communicated. Further, the mechanisms should be easy to use, provided through appropriate channels, and free to end users.

The Inclusive IPS should also provide tools to DFSPs that support initiation of an investigation and request of funds in cases of confirmed fraud.

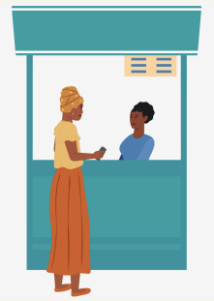
Example: The Special Mechanism for Return [of Funds] provided by Brazil's Pix.

Complaints may result in a dispute. **Fraud dispute resolution processes** enable parties involved in the dispute to arbitrate whether a transaction is fraudulent. Effective fraud dispute resolutions require clear rules and procedures to determine if fraud was present (the burden of proof sits with the DFSP), and mechanisms for timely return of funds to the end user. The rules for funds return should be clear on timelines. Consideration should be given to immediate funds reimbursement.

An independent dispute arbitrator (Ombudsman) and process should provide a secondary mechanism for addressing disputes that are not adequately resolved at the DFSP level. The Ombudsman role may be played by various entities, such as the central bank, consumer protection authority, or a body with representation from various entities that are not selected by and do not include the DFSPs. The independence of the body must be assured through a rigorous process for structuring its governance, selecting representatives, and designing the dispute process. The Ombudsman's role should be made known to the end users and its dispute process easy to access, user friendly, and efficient.

The Inclusive IPS should advocate for and collaborate with ecosystem stakeholders to put such a body in place and ensure its independence.

Example: India's NPCI provides guidelines and tools to enable end user complaints as well as a multi-layered resolution mechanism that includes an Ombudsman.



Guidance 15: Data Reporting

Rules | Data

The Inclusive IPS mandates participants to submit ON- and OFF-US transactions to the scheme and report confirmed fraud to the scheme, which will use the data for permitted purposes, including fraud mitigation.

The robustness and effectiveness of Inclusive IPS fraud tools depend on availability of transaction data. For Inclusive IPS tools to develop transaction screening rules and apply them to the identification of transactions that are suspicious, a baseline needs to be established over time using transaction data, inclusive of all transactions (ON- and OFF-US, non-fraudulent and fraudulent).

Data sharing needs to align with data protection regulations, which often allow exceptions for fraud mitigation. As such, the Inclusive IPS should only use the data for fraud mitigation purposes.

Example: Both the FedNow and Pix systems include a requirement for DFSPs to report fraudulent payments.

THE LEVEL ONE PROJECT

Section 5

Ecosystem Fraud Mitigation Initiatives

Partner Initiatives in Fraud Mitigation

The L1P fraud mitigation lens will add to the body of work contributed by multiple global and local partners, including NGOs, providers, regulators, and others, toward Inclusive IPS ecosystem fraud risk mitigation. Illustrative initiatives are highlighted below.

GSMA Certification

The GSMA Mobile Money Certification is a global initiative to bring safer, more transparent, and more resilient financial services to millions of mobile money users around the world. It is based on independent assessments of a provider's ability to deliver secure and reliable services, to protect the rights of consumers, and to combat money laundering and the financing of terrorism.

Better Than Cash Alliance

UN Principles for Responsible Digital Payments

World Bank

Financial consumer protection encompasses the laws, regulations, and institutional arrangements that safeguard consumers in the financial marketplace. World Bank offers resources that include technical guidance, country reports, and tools for policymakers, regulators, development partners, and other experts.

Collaborative efforts between global and local partners are crucial to combat digital financial services fraud. Their combined and unique expertise ensures comprehensive strategies, regulatory alignment, and shared intelligence that leads to sustaining trust in digital financial services while reinforcing safeguards against evolving threats.

Ashley Olson Onyango
Head of Financial Inclusion & AgriTech
GSMA

FRMS Center of Excellence and OSS Engine

In many geographies, only top-tier, well-funded organizations can afford to have the tools they require to reduce fraud, money laundering, terror financing, and other types of financial crime.

Other organizations do not have adequate budgets to allocate to risk mitigation solutions or lack the expertise to implement and operate a complete solution.

As a result, many smaller digital financial service providers (DFSPs) are constrained in their ability to be able to reduce fraud and other types of financial crime.

The Fraud Risk Management System Center of Excellence (FRMS CoE) is an organization being built out with the purpose of reducing the risk and cost of fraud.

At the heart of its mission will be to act as a trusted source of fraud risk education, expertise, and the governance and advocacy of its own free open-source fraud monitoring software.

The FRMS CoE provides an open-source transaction monitoring solution (TMS) in support of fraud risk management.

The TMS is one example of a shared utility built to support DFSPs and Inclusive IPSs in raising the bar on fraud risk management.

- **Preconfigured with 30+ customizable Inclusive IPS fraud typologies**
- **Implementable by organizations across financial ecosystems**
- **Designed for low-cost operation**
- **Architected for any size of organization**
- **Flexible, and works in concert with other components of a fraud risk program**

Digital payments systems are essential in driving financial inclusion. Our vision is to build trust in instant payments by protecting those who can least afford to lose money because of fraud.

Greg McCormick

Executive Director
Fraud Risk Management Systems Center of Excellence

More information: https://frms.io/

THE LEVEL ONE PROJECT

Section 7

Appendix

6

Summary of Design Guidance

	Tenets	Liability	Rules	Tools	Data
Cross-Cutting	1 The Inclusive IPS provides a framework for defining fraud types.	•		•	•
	2 The Inclusive IPS leads and participates in collaborative efforts to define and evolve a fraud typologies catalog. The catalog is made available to DFSPs for use in transaction screening.			•	•
	3 The Inclusive IPS considers payments that have been authorized as a result of social engineering, in which the legitimate end user is not complicit, to be fraudulent.	•			
	4 The Inclusive IPS requires DFSPs to apply controls appropriate for each KYC tier and customer risk profile.		•	•	•
	5 The Inclusive IPS provides guidelines for confirmed fraud reporting and safe use of data to protect end user privacy and DFSP data confidentiality.		•		•
Before Payment	6 The Inclusive IPS requires DFSPs to utilize multiple tools and controls to authenticate end users.		•		
	7 The Inclusive IPS enables a confirmation of payee (CoP) service that allows end users to verify the name of the receiver prior to initiating a payment.		•	•	
	8 The Inclusive IPS requires DFSPs to implement controls designed to prevent a DFSP employee from perpetrating fraudulent payments.		•		
	9 The Inclusive IPS requires DFSPs to utilize clear and descriptive account-naming conventions.		•		
	10 The Inclusive IPS requires DFSPs to educate end users, employees, and partners on fraudster tactics and mitigation practices on an ongoing basis and at payment initiation using proven approaches.		•	•	
Payment Phase	11 The Inclusive IPS requires DFSPs to monitor for suspicious transactions and be capable of preventing potentially fraudulent transactions while minimizing the impact on legitimate transactions.		•	•	•
	12 The Inclusive IPS provides a shared fraud utility tool, designed to identify, prevent, and respond to potentially fraudulent transactions while minimizing the impact on legitimate transactions.			•	•
	13 The Inclusive IPS provides DFSPs with the capability to submit a list of bad actors, which allows the scheme to screen transactions against the list, and to reject any that trigger the list.			•	•
	14 The Inclusive IPS provides a safe payments-addressing approach.			•	
After Payment	15 The Inclusive IPS requires DFSPs to provide complaint and dispute resolution mechanisms that are clearly communicated, easy and free for end users, and appropriate to the local context.	•	•		
	16 The Inclusive IPS mandates participants to submit ON- and OFF-US transactions to the scheme and report confirmed fraud to the scheme, which will use the data exclusively for fraud mitigation purposes.		•		•

The Level One Project

Gates Foundation

The Level One Project is an initiative of the Gates Foundation's Inclusive Financial Systems (IFS) program, which is part of the Global Growth and Opportunity division.

Inclusive Financial Systems

FSP's Objectives

Increasing poor people's capacity to weather financial shocks and capture income-generating opportunities.

Generating economy-wide efficiencies by digitally connecting large numbers of low-income consumers with those whom they transact.

Level One Project

The Level One Project enables these objectives by working to support inclusive, interconnected digital economies to bring poor people into the global financial system, and ultimately to help promote global growth and opportunity.

Working across the public, private, and nonprofit sectors in coordination with a wide variety of institutions, the Level One Project is a multiyear effort to address digital payments system infrastructure at a national and regional level, and do so in a way that's both sustainable and compelling for providers of financial services.

A Vision

A vision for inclusive instant payments systems that support low-cost, interoperable digital economies, and the design principles to achieve this.

A Blueprint

A blueprint for how such a system could be configured within a country or region.

A Set of Resources

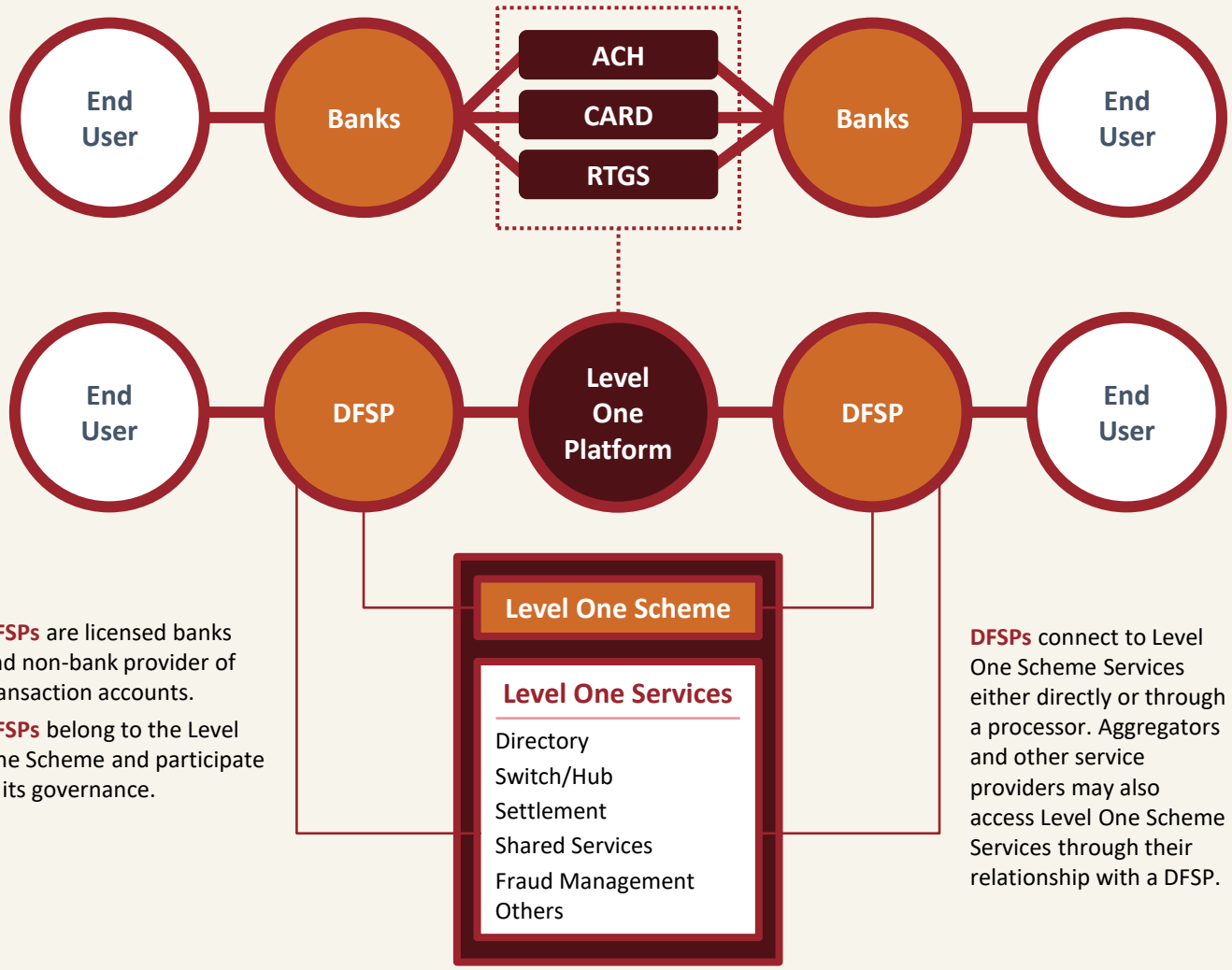
A set of tools and resources to enable the implementation of inclusive instant payments systems that are Level One aligned.

The Level One Core Components

A Modern Digital System to Reach and Serve the Excluded

A Level One aligned system is a digital system to facilitate immediate and real-time digital payments. It enables users—individuals and merchants—excluded to be reached and served in the formal financial ecosystem. The system exists along with—and among—other payments systems in the country or region.

A Level One Platform is payment platform that reflects the design principles of the Level One Project. Many are being referred to as "RTRP" (real-time retail payments) or as "Faster Payments" platforms in some countries.



DFSPs are licensed banks and non-bank provider of transaction accounts.

DFSPs belong to the Level One Scheme and participate in its governance.

DFSPs connect to Level One Scheme Services either directly or through a processor. Aggregators and other service providers may also access Level One Scheme Services through their relationship with a DFSP.

More Information: Scaling the system