Febelfin action plan against online fraud

Executive summary

Febelfin and its members fully share the concerns regarding the growing impact of online fraud on consumers and society as a whole. Online fraud has evolved into a structural and rapidly changing societal challenge, driven by digitalization, technological innovation, increasingly sophisticated social engineering techniques and the industrialisation of criminal networks.

Over the past years a marked increase in both the scale and the sophistication of fraud attempts has been observed. In response, **banks have made significant and sustained efforts to strengthen fraud prevention, detection and customer protection**. These efforts span the entire fraud lifecycle, from prevention and continuous transaction monitoring to operational security measures, cooperation with police and judicial authorities, and ongoing awareness-raising initiatives aimed at customers.

These efforts have increased materially in recent years (IT development capacity, fraud-related staffing, …) showing the financial sector is fully committed to further strengthening its role in the fight against online fraud. Banks will continue to scale up their technical and operational security measures, deepen cooperation between banks and other relevant actors, with the necessary political and regulatory support, and further improve customer support in the event of fraud. At the same time, the sector recognises that banks cannot address this challenge alone.

Online fraud cannot be effectively tackled through a bank-centric approach. A sustainable reduction in fraud requires **an integrated and coordinated approach in which all actors involved in the fraud chain assume their responsibilities**, with public authorities playing a key coordinating and facilitating role. Fraud must be addressed as close as possible to its source, notably through closer cooperation with telecom operators and social media platforms, and through effective investigation and prosecution to deter organised criminal networks. As in neighbouring countries, a collective and structured response is essential to combat this form of organised crime. Together, we must avoid making Belgium an attractive destination for fraudsters.

Belgian Financial Sector Federation vzw/asbl
Boulevard du Roi Albert II 19 - 1210 Brussels
http://www.febelfin.be | T + 32 2 507 68 11 | F + 32 2 888 68 11
Governance Note FEB559746
Last saved on 7/07/2026 15:38:00 – 21 pages

Against this backdrop, Febelfin and its members propose a comprehensive action plan structured around three complementary levels.

1. **Banks commit individually to take operational and technical protection measures, aimed at further strengthening prevention, detection, and response mechanisms. This means the introduction of some slow banking measures, while maintaining a sufficient proportionate balance between security and usability.**
2. **Banks will enhance interbank cooperation**, moving towards a more integrated approach based on intelligence and data sharing and common technological capabilities. The financial sector also commits to more harmonized and client-centric customer handling and joint awareness raising.
3. **Banks call for a full ecosystem approach**, recognizing that fraud often originates upstream—via telecom operators, social media platforms and digital channels—and requires stronger involvement and accountability of other actors, as well as effective law enforcement.

This three-level approach, which will require **broad societal acceptance and regulatory support**, is designed to strengthen **customer protection**, improve operational effectiveness, and align with the evolving European regulatory framework, notably the Payment Services Regulation (PSR). It also highlights the need for **strong political support** to enable data sharing, ensure cross-sector accountability, and avoid regulatory fragmentation. Ultimately, only a **coordinated effort across the entire ecosystem** can deliver a sustainable and lasting reduction in online fraud.

Introduction: the current fraud landscape

Febelfin and its members take the fight against online fraud extremely seriously. The sector is fully aware of the financial, emotional, and societal impact fraud has on victims. On a daily basis, banks invest significant resources to prevent fraud, detect suspicious activity, block fraudulent transactions, support victims, recover funds where possible, and cooperate closely with public authorities and law enforcement. These efforts are continuously adapted to emerging fraud patterns and evolving threats.

Despite these sustained efforts, online fraud continues to cause **substantial harm**. In 2025, fraudsters have succeeded in extracting 93 million euro through phishing, illustrating both the persistence and the adaptability of criminal networks.

At the same time, it is important to place online fraud in its broader transactional context. Out of a total transaction volume, the net loss amount related to fraud represents approximately 0.004% of the total transaction amount (2025). These figures show that fraudulent transactions remain very limited in relative terms, but they also underline the significant impact that fraud can have on individual victims and the need for continued and proportionate efforts to further strengthen protection, as every victim is one too many.

Online fraud has fundamentally changed in nature. **It is an ecosystem-wide phenomenon involving multiple actors across the fraud chain.** Criminals operate in an increasingly structured and industrialized way, often across borders, using phishing kits, fake websites, mule accounts, call centers, scam farms, social media advertisements, remote access tools and artificial intelligence. Telecom operators, social media platforms, marketplaces and other digital channels are frequently used upstream to identify, contact and manipulate victims.

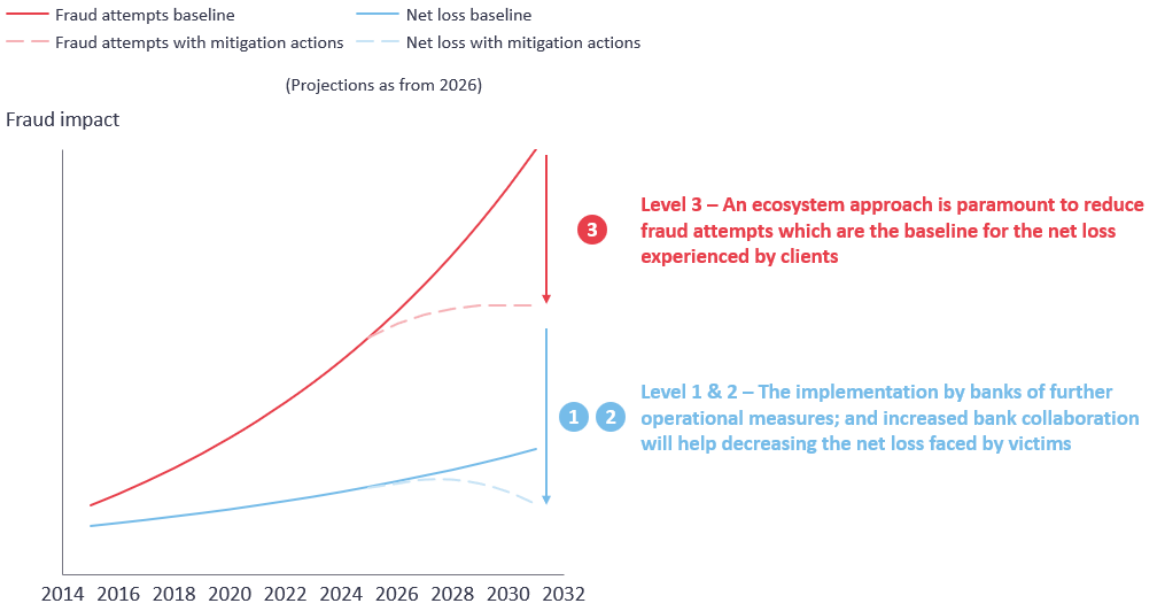
Banks, by contrast, are primarily involved downstream. They execute and monitor payment transactions, implement preventive and detective controls, block payment instruments where needed, initiate recovery actions and support customers after fraud has occurred. This downstream role is critical, but it also means that **banks have limited control over the initial stages of the fraud chain**, where victims are first contacted, manipulated and prepared before a payment is initiated.

Banks have already **implemented a broad and robust set of operational and technical measures** to protect customers against online fraud. These measures span the full fraud lifecycle and can be understood through their distinct but complementary impact on fraud dynamics. **Prevention** measures (such as strong customer authentication, itsme® and payee verification) contribute to limiting fraud by making attempts more difficult to execute. **Detection and mitigation measures** (including transaction monitoring, blocking suspicious transactions, alerts and recovery processes) primarily reduce the financial impact of fraud by limiting losses once an attempt has been successful.

These measures have already delivered tangible results in strengthening customer protection. By continuously enhancing prevention, detection and response capabilities, banks have significantly

improved their ability to identify suspicious transactions, intervene in real time, and limit financial losses for customers. Banks remain fully committed to further reinforcing these efforts, including through additional operational safeguards, technological innovation and strengthened cooperation within the sector. These continued investments will contribute to further reducing the financial impact of fraud and improving the protection of victims.

However, the evolution of fraud dynamics, as illustrated in the chart below, highlights that these measures primarily influence the **impact of fraud once it occurs**, rather than the **overall volume of fraud attempts**. Even with further improvements at bank level, their ability to structurally reduce the number of attacks remains inherently limited, as fraud is largely initiated upstream through channels outside the banking sector. **A sustainable and significant reduction in fraud therefore depends to a large extent on effective action by the broader ecosystem** — notably telecom operators, social media platforms, digital service providers, and law enforcement authorities — to prevent, detect and disrupt fraudulent activities at their source. Strengthened bank measures are necessary, but only a coordinated ecosystem approach can materially alter the trajectory of fraud attempts.



The evolution of fraud is closely linked to broader digital trends. The rapid adoption of digital and mobile banking, instant payments and digital-first customer behavior has increased convenience for consumers but has also created new vulnerabilities. Fraudsters exploit these vulnerabilities by shifting from mass phishing to more personalized attacks, using advanced data collection, artificial intelligence, deepfake voices and convincing multilingual phishing messages.

Increasingly, fraudsters target customers directly, exploiting trust, urgency and manipulation to induce victims to disclose credentials, approve transactions or increase transfer limits themselves. In such cases, the bank does not immediately see “fraud” at the moment of execution, but rather a transaction that appears authorised by the customer. These fraud attempts where victims are manipulated into approving transactions themselves, are becoming increasingly important because it can bypass traditional technical security measures. This evolution is crucial to understand both the technical limits of bank-level controls and the necessity of a broader, integrated approach to address fraud at its source (see attachment for two examples of the “fraud journey” for most frequent modus operandi).

This landscape clearly demonstrates the need for a multi-layered response. Banks must continue to strengthen their own controls, but a bank-centric approach alone will not be sufficient. **Fraud must be addressed throughout the entire chain**, through stronger prevention upstream, better data sharing, clearer responsibilities for other sectors, improved law enforcement, more coordination, and a coherent national approach.

Against this background, Febelfin proposes an ambitious but operationally realistic action plan, under which banks take significant additional commitments while explicitly calling for a coordinated and integrated approach across the entire ecosystem. **The objective is to further protect customers, enhance the effectiveness of fraud prevention and response, and ensure full alignment with the current and future European regulatory framework**, including PSD2, the Instant Payments Regulation and the forthcoming Payment Services Regulation. National initiatives should remain consistent with this European framework and gold plating should be avoided.

Febelfin action plan level 1 – Operational and technical measures taken and further strengthened by individual banks

Banks have already **implemented a broad and robust set of operational and technical measures** to protect customers against online fraud.

Over recent years, the efforts of banks have been continuously strengthened through increased **human and technological resources**. Banks have expanded both IT development capacity and specialised fraud teams, reflecting the structural nature of the threat and the need for constant adaptation to evolving fraud patterns.

Building on the measures already implemented by individual banks in line with their respective customer bases and risk assessments, **banks commit to further reinforcing their individual frameworks through a set of aligned operational measures.** The aim is to establish a **common baseline across the sector**, with a **minimum set of operational measures** to which the banks commit. Banks will also implement and continue to complement these measures based on their own risk profile and the specificities of their customer segments, taking into account the intended timing for each measure.

The measures proposed are designed not only to **strengthen technical protection**, but also to deliberately **introduce moments of pause and reflection** in the transaction process where this can help **disrupt fraud scenarios**. By **slowing down** certain high-risk steps — for instance through cooling-down mechanisms — and by increasing customer awareness via targeted alerts and confirmations, banks aim to **break the fraud chain at critical points.**

These measures address the key characteristics of modern fraud — urgency, manipulation and high-value transfers — while seeking to maintain a proportionate balance between security, usability and customer autonomy.

The Febelfin action plan contains following operational measures by individual banks aiming at:

Preventing online fraud:

1. **Lower standard limit (5,000 EUR/day) for credit transfers from payment accounts for retail customers**
2. **Cooldown period (>4h) for limit increase**
3. **Notification in case of limit increase**
4. **Contextual signing**[1]
5. **Customer choice between instant and standard credit transfers**
6. **Limit fraudulent transactions on savings accounts**

Detection & treatment of online fraud:

7. **Strengthening fraud detection and transaction monitoring**
8. **Malware & Remote access tool (RAT) detection**

Preventing online fraud:

1. Lower standard limit (5,000 EUR/day) for credit transfers from payment accounts for retail customers – mitigating financial exposure

number of banks that apply already today the lower standard limit
(based on a sample of 10 retail banks, 4/10)

Banks will **lower standard credit transfer limits from payment accounts for retail customers to a maximum of 5,000 EUR/day.** A lower default ceiling **reduces the maximum financial exposure per fraud event,** especially where losses are driven by high-value single transactions. By lowering the standard limits, the amount that fraudsters can loot without increasing the limits is greatly reduced. Customers will still be able to request increases, but such increases will be subject to controlled processes and additional safeguards (see cooldown period and notifications).

The standard limit of 5,000 EUR/day is a maximum. A bank can always decide to implement a stricter default limit (e.g. 4,000 EUR/day or 5,000 EUR/week). It is equally important to note that also the customer can further decrease its personal limits, lower than the standard limit set by the bank.

Target timing: Q1 2027

[1] Contextual signing guarantees that the transaction details which are displayed to the rightful signer (including amount and full beneficiary IBAN) are the same as the transaction details which are executed. This includes signature means directly linked to a device such as face ID / fingerprint on mobile and passkeys.

2. **Cooldown period (>4h) for limit increase – Introducing a delay and disrupt to fraud scenario's**

number of banks that apply already today the cooldown period
(based on a sample of 10 retail banks, 5/10)

Banks will **introduce a cooldown period (of at least 4h)** for credit transfer limit increases. Under this measure, a request to increase a customer's transfer limit through digital channels will not take effect immediately. Instead, the previous lower limit will remain active during at least 4h. This is designed to **disrupt fraud scenarios** that rely on urgency and immediate execution after a limit increase.

Target timing: Q4 2026, with careful calibration to limit friction for legitimate urgent payments.

3. **Notification in case of limit increase – A second line of defense enabling rapid detection**

number of banks that apply already today the notification in case of limit increase
(based on a sample of 10 retail banks, 7/10)

Banks will introduce **systematic real-time notifications when transfer limits are increased** (and when the cooldown period has ended). This provides an additional safeguard by immediately alerting the customer to a change that may have been initiated under manipulation. Notifications should be clear, practical and action-oriented (what changed, when, and what to do if the customer did not request it).

Target timing: Q2 2027

4. **Contextual signing - reduce fraud risk**

number of banks that apply already today contextual signing
(based on a sample of 10 retail banks, 4/10)

Banks will further strengthen the way customers confirm transactions by ensuring they see clear, transaction-specific information at the moment of approval (such as amount and beneficiary details). This helps customers **understand exactly what they are authorizing** and reduces the risk that they unknowingly approve a fraudulent transaction under manipulation.

Implementation will be **gradual across 2026- 2027**. This measure is combined with the gradual phasing out of non-contextual card readers, while maintaining the possibility to continue using such card readers for customers who wish to do so.

5. Customer choice between instant and standard credit transfers - reduce fraud risk

number of banks that apply already customer choice between instant and standard credit transfer
(based on a sample of 10 retail banks, 10/10)

Banks will ensure that customers always retain the ability to choose between an instant credit transfer and a standard (non-instant) credit transfer. Since October 2025, all banks in Europe are obliged to offer their clients Instant Payments. Instant payments, which allow funds to be transferred to the beneficiary within seconds, are increasingly popular due to their speed and convenience. At the same time, this immediacy can be exploited by fraudsters to move funds away from victims' accounts very rapidly once manipulation has occurred.

To address this risk, **banks will always offer customers the option to use a standard credit transfer**, whereby funds are not immediately credited to the beneficiary.. This additional time window can help disrupt fraud scenarios that rely on urgency and pressure, and may allow suspicious situations to be detected or reassessed before irreversible harm occurs.

This **customer choice** can be implemented through different operational set-ups, depending on the bank's service model:

- the bank may offer the standard credit transfer as the default option, with the customer explicitly opting for an instant payment where desired;
- the bank may offer the instant payment as the default option, while allowing the customer to switch to a standard credit transfer; or
- the bank may require the customer to actively choose between an instant and a standard credit transfer for each transaction.

In all cases, the customer remains fully in control and can consciously decide which transfer option best suits their needs. This measure aims to combine convenience with protection, by introducing a **deliberate and informed choice** that can help **slow down fraud scenarios and break the fraud chain**, while preserving a proportionate balance between speed, security and usability.

Target timing: immediately (Q2 2026)

6. Limit fraudulent transactions on savings accounts – reduce fraud risk

number of banks that apply already measures to limit fraudulent transactions on savings accounts
(based on a sample of 10 retail banks, 2/10)

Banks will take additional measures in order to limit fraudulent transactions on savings accounts. These measures can be:

- offer retail customers the option to limit and/or block online transfers from their regulated savings accounts to their current accounts — as part of a 'Slow Banking' approach — combined with a secure alternative (e.g. in-branch processing or a complementary cooling-off period) to authorize such transactions and/or
- implement a dynamic "on hold" option based on transaction monitoring.

Target timing: Q3 2027

Detection & treatment of online fraud:

7. Strengthening fraud detection and transaction monitoring

Banks will further strengthen their measures to detect and prevent fraudulent transactions by **enhancing their fraud detection and transaction monitoring capabilities**. Advanced monitoring mechanisms enable banks to identify suspicious patterns and, where appropriate, to intervene in a timely manner by blocking or suspending potentially fraudulent transactions before irreversible harm occurs. At the same time, it is essential that an **appropriate framework is in place to address potential legal or regulatory obstacles** that could limit the use of effective fraud-detection tools, such as behavioural transaction monitoring based on advanced analytical techniques. Technological innovation can be a powerful instrument in the fight against online fraud and should be enabled, provided it is deployed in a responsible and proportionate manner.

Banks therefore underline the importance of allowing such innovation within a **clear and legally secure framework** that fully respects applicable privacy and data-protection rules. Ensuring the right balance between effective fraud prevention, technological progress and the protection of fundamental rights is key to strengthening customer protection and disrupting fraud scenarios across the transaction chain. Implementation will be **gradual across 2026-2028**.

8. Malware & RAT detection – Targeting the most advanced fraud techniques

number of banks that use already malware and/or RAT detection
(based on a sample of 10 retail banks, 4/10)

Banks will further explore mechanisms (e.g malware and remote access tool detection) to detect compromised customer sessions (e.g., when a customer's device is being remotely manipulated). This is an important area to address more advanced fraud techniques. It requires careful development and calibration, notably to minimise false alerts and ensure a proportionate customer experience. **Implementation will be gradual across 2026-2028**.

Finally, online fraud is an evolving phenomenon that requires continuous monitoring, with best practices being constantly identified, assessed and implemented where proven effective in combating online fraud. Inspiration can also be drawn from abroad, where certain tools or measures are sometimes introduced that are not always rooted in European regulation. Febelfin is committed to using benchmarking to identify and evaluate new features and to recommend their adoption by its members where they are proven effective and gain broad support across the sector.

For all these technical and operational measures aimed at introducing a degree of "slow banking", an important consideration regarding customer experience should be highlighted: while these measures will improve protection, they may also introduce additional steps or delays for certain transactions. Febelfin therefore stresses the importance of broad societal and political support. Stronger protection measures can only be effective and sustainable if customers, policymakers and regulators recognize that a higher level of security may require certain adjustments in terms of speed, convenience and user experience.

Febelfin action plan level 2 – Interbank collaboration

Individual bank-level measures are necessary, but not sufficient. Online fraud often involves multiple banks across the transaction chain, particularly when funds are transferred through mule accounts or moved rapidly across institutions and jurisdictions. Strengthened interbank collaboration is therefore essential to detect fraud earlier, block funds faster, improve recovery and provide victims with a more consistent and client-centered experience.

The Febelfin action plan contains following measures through interbank collaboration aiming at:

Preventing online fraud:

1. **Fraudstop**
2. **Awareness campaigns**
3. **Itsme ®**

Detection & treatment of online fraud:

4. **Fraud data sharing platform**
5. **Communication charter – a commitment from the banking sector to handle fraud cases within 15 business days**

Preventing online fraud:

1. Fraudstop – a single, easily 24/7 accessible reporting entry point

Victims often face uncertainty in the first minutes after discovering fraud: whom to call, which procedure to follow, and what to do first. Therefore, the sector developed Fraudstop, a **single entry point with a unique number (078 170 170)** that is reachable at any time of the day and the week; and routes victims quickly to the relevant bank and immediate protection actions (including blocking payment means where needed). This initiative builds on the strength and public familiarity of the existing 24/7 sector service, Card Stop, and aims to make victim support simpler and faster. Next to this new entry point, each bank will remain available through its existing fraud contact channels.

Timing: launched 22 June 2026

2. Awareness campaigns – recurring communication towards the public

At first, banks will continue to invest in awareness campaigns. Since human behavior and social engineering are at the core of many online fraud scenarios, prevention also depends on making customers more resilient. Awareness initiatives should be recurring, targeted, and adapted to the relevant fraud modus operandi and communication channels. Ideally, awareness raising is a joint effort of the entire ecosystem to increase the impact and scale of the initiatives taken. Banks support

the idea of the development of large-scale awareness campaigns, similar to the well known “Bob campagnes”.

Target timing: recurring

3. itsme® will strenghten its fraud prevention measures

Over the last 8 years, itsme® has been continuously adding datapoints, as well as specific mitigations in close concertation with the banks to improve fraud-resistance. Some are covered through a direct integration with the banks and signals exchanged there, some of these innovations are quite visible to the users themselves and create instant, contextual, awareness.

As part of these initiatives, itsme® will be adding extra layers of security via itsme® and innovations in mobile apps. This will reduce the risk of accounts being taken over, and stop fraudsters from confirming a login or payment on behalf of their victims. Only the genuine user matching the picture on his or her Belgian identity card will be able to act as the account holder, which adds a barrier that fraudsters cannot get past.

Target timing: Q1 2027

Detection & treatment of online fraud:

---

4. Fraud data sharing platform – a network-based intelligence

An important key initiative is the development of a fraud data sharing platform via Isabel and itsme®.

Banks want to share signals about fraud faster and in a more structured way, so that suspicious patterns can be recognized and stopped earlier. The objective is to move from isolated detection to network-based intelligence. By sharing relevant fraud indicators, banks can detect mule activity earlier, avoid further fraudulent transactions and coordinate their response more effectively. In this context, the further development of the Fraud Data Sharing platform will be key, including the integration of additional fraud indicators, such as signals originating from the citizen’s mobile device.

In the short term, the platform will consist of the creation of mule data sharing; in the mid/long term the ambition is to broaden the scope with multi-source signals (telco/devices/ itsme®).

This initiative is aligned with national priorities and with the direction of the future European regulatory framework, which increasingly recognizes the importance of fraud-related information Such initiatives require **legal certainty** and an appropriate framework, notably to ensure that data exchange is safe, proportionate and compliant. Political support, together with the active involvement of supervisors (e.g. Data Protection Authority), is therefore essential to enable effective cooperation and avoid gaps that criminals can exploit. It remains crucial in this regard for banks to be able to assess a (new) client relationship with the identified fraudster(s) in line with applicable (AML, PAD …) legislation.

After all, banks have been asking for more fraud data sharing for years. To date, only the banks directly involved in a fraud case are allowed to exchange information on a bilateral basis (money mule data). This information cannot be shared with another bank, making it much more difficult to really stop fraudsters and money mules. More cooperation will lead to an even more efficient fight against fraud.

Target timing: pilot phase Q1 2027

5. **Communication charter – a commitment from the banking sector to handle fraud cases within 15 business days**

A third priority is the harmonization of customer communication and case handling. The sector commits to handling fraud cases within a maximum of 15 banking business days[2]. It will be supported by dedicated fraud-handling workflows, standardized processing timelines and integration within a sector-wide communication charter. The measure is also aligned with the future PSR framework.

The communication charter will translate these commitments into clear and consistent customer experience. Its core principles include acting fast, ensuring reachability 24/7, protecting the customer first, keeping the customer informed, guiding the victim step by step, working with the police and ensuring consistent support regardless of the reporting channel. With this Charter, the banks want to commit to ensuring that their customers who have become victims of online fraud receive the right information and necessary guidance, paying attention to their individual file.

Target timing: Q4 2026

[2] Although if foreign banks are involved in the fraud case, this 15 days might be exceeded.

Febelfin action plan level 3 – Ecosystem approach

In this context, it is important to underline that banking measures alone — whether at individual or sector level — cannot deliver lasting results in the absence of a fully functioning ecosystem approach. Without effective action by other public and private actors upstream and downstream in the fraud chain, additional banking safeguards risk merely mitigating the consequences rather than addressing the root causes of fraud. We refer to examples like in the UK or the Netherlands.

Moreover, a coordinated ecosystem approach is essential to avoid the emergence of regulatory or operational asymmetries that could make Belgium an attractive target for fraudsters. If fraud is addressed unevenly across the chain or across jurisdictions, there is a real risk that criminal activity will gravitate towards the weakest link. Banks are prepared to further strengthen their own measures, but this can only be effective if all actors — public and private — take complementary and coherent action to tackle fraud at every stage of the chain.

Febelfin asks that the government takes the following measures:

1. **Strengthen the role of the CCB as central coordinator**
2. **Increase accountability of telecommunication companies and social media platforms**
3. **Stronger law enforcement impact (police and justice)**
4. **Strengthening strong customer authentication (SCA) in online transactions ('soft decline')**
5. **Government as facilitator: adjust the legal framework where necessary**
6. **European alignment and avoidance of fragmentation & gold plating**
7. **Supporting joint awareness campaigns**

1. Strengthen the role of the CCB as central coordinator

Febelfin calls for a genuine ecosystem approach, coordinated by public authorities and involving all relevant private and public stakeholders. The Centre for Cybersecurity Belgium (CCB) is the authority in the field of cyber security in our country. To make this approach effective, two priorities should be pursued:

- **The development of a national anti-fraud plan**, to which the banks will actively contribute. Such a plan is required to align priorities, avoid fragmentation and ensure that prevention, detection, reporting, investigation and enforcement are addressed in a coherent way.
- The role of the CCB should be strengthened as a **central coordinator**, by chairing a centralized coordination platform that brings together all relevant public and private stakeholders to drive the implementation of the national anti-fraud plan and ensure effective cooperation.

2. Increase accountability of telecommunication companies and social media platforms

Telecom operators and social media platforms play a central role in the early stage of online fraud and must assume (more) their responsibilities. Telecom channels are frequently used for fraudulent calls and messages, while social media platforms and advertising environments are used to distribute scam ads, impersonate trusted actors and recruit money mules. These actors hold important signal data and have prevention capabilities that can help stop fraud upstream. Their responsibilities should therefore be clarified and strengthened, in line with the broader “shared responsibility” approach.

For social media platforms and Big Tech, this includes faster detection and removal of fraudulent advertisements, accounts and scam content, as well as clear accountability in line with the Digital Services Act and the future PSR framework. The possibility of designating trusted flaggers to report fraudulent advertisements should also be assessed within the existing legal framework.

For social media platforms and telecom operators, enhanced cooperation should also include the establishment of mechanisms to share relevant fraud-related information with banks in accordance with the future PSR. In this respect, additional or further legislative initiatives or clarifications may be necessary to provide a robust legal basis for these data exchanges, ensure legal certainty across sectors, while safeguarding data protection principles, and enable effective, coordinated action against fraud.

In particular, telecom operators could play a pivotal role through the development of data-sharing interfaces with banks and itsme®, enabling the exchange of fraud-relevant signals such as SIM swap indicators, line-busy signals, suspicious numbers or certain communication metadata. Such exchanges should take place within a clear, proportionate and legally robust framework. Strengthening this collaboration would significantly improve early detection at the transaction stage and enhance visibility across the entire fraud chain.

Stricter supervision and requirements for telecom operators and social media platforms is needed to enforce their obligations:

- It is incomprehensible that a person manages to buy hundreds of SIM cards with the identity card of a family member. Such facts can indicate fraud and should therefore be dealt with decisively by the telecom operators in line with the end-user identification requirements imposed by Belgian law.
- Similar concerns arise in the context of the current port-out process. At least with some operators, a fraudster can take over another person's phone number based solely on the customer number linked to that person's telecom account, which can be relatively easy to obtain through phishing. The fraudster can then request a SIM swap and have a new SIM card delivered to an address of their choosing. Such shortcomings illustrate the need for stricter supervision and stronger controls, as they not only facilitate fraud but also raise serious KYC and customer identification concerns.

- Reports show that social media platforms make a business model on fraudulent adds[3]. These platforms should take down fraudulent websites in line with the European Digital Services Act.

3. Stronger law enforcement impact (police and justice)

Banks also expect stronger and more structured collaboration with police and justice, as law enforcement and the judiciary play a decisive role at the end of the fraud chain. While banks can prevent, detect, block transactions and initiate recovery actions, only police and judicial authorities can investigate criminal networks, prosecute offenders and dismantle the organized structures. This is particularly important given that fraud is increasingly organized, cross-border and industrialized, with funds often routed through mule accounts, multiple banks, crypto-assets or foreign jurisdictions.

Febelfin therefore calls for reinforced national coordination with police, prosecutors and courts, supported by adequate resources, specialized expertise and faster information flows between banks and law enforcement. Such cooperation should move beyond isolated case-by-case handling and enable a more strategic approach focused on identifying patterns, tracing money flows and targeting the higher-level criminal organizations behind fraud schemes. A pilot collaboration with the prosecutor's office, for example, could help focus enforcement efforts on dismantling organized fraud networks rather than only addressing individual incidents. The police and the Public Prosecution Service should have access to the (future) fraud data sharing platform and should also feed it. This stronger judicial and law enforcement response is essential to complement preventive measures taken by banks and to ensure that the fight against online fraud addresses not only victim protection, but also the criminal source of the problem.

Febelfin expects the government to invest the necessary resources in the police and the judiciary. A lax prosecution policy due to a lack of resources leads to impunity for the perpetrators and acts as a magnet for potential fraudsters and criminals. This is essential both to deter criminals and to reduce the sense of impunity for victims.

4. Strengthening strong customer authentication (SCA) in online transactions ('soft decline')

The banks will take initiative (via sector-wide agreement and/or via request to the regulator) to make SCA mandatory for certain online transactions (the so-called SCA card not present (CNP) transactions, according to the French measure).

The PSD2 directive provides for exceptions for the use of SCA in online transactions. In the case of, for example, known beneficiary, small amounts with limited risk,... SCA is not required. These exceptions are often a cause of many cases of fraud (often for relatively small amounts). By applying the 'soft

[3] https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/

decline' mechanism (the payment request without SCA is rejected but the merchant/seller can resubmit the payment request with SCA) this problem can be largely solved.

5. Government as facilitator: adjust the legal framework where necessary

Some banking measures can only be implemented if certain legislation is enforced and/or amended within a reasonable timeframe:

- Fraud data sharing: exchange of money mule data between banks (name, national register number).
- Exchange of telco metadata (eg whether the call is active, length of the call,...)
- Use of biometric data in behavioural transaction monitoring (individual profiling) in the context of fraud detection.
- Social media platforms must quicker remove fraudulent advertisements and be held legally accountable in accordance with the EU DSA (Digital Services Act) and the PSR.
- It must be assessed who can be designated as a trusted flagger under this legal framework to submit reliable reports of fraudulent advertisements
- Telecom operators must respect the end-user identification requirements imposed by Belgian law.

6. European alignment and avoidance of fragmentation & gold plating

This three-level approach is designed to strengthen customer protection while remaining consistent with the evolving European regulatory framework. The sector stresses the importance of alignment with EU rules and the need to avoid national gold-plating or fragmented initiatives that reduce legal certainty and operational effectiveness

7. Supporting joint awareness campaigns

Awareness-raising campaigns are an essential element in fraud prevention. The banking sector is committed to a common communication approach and will develop a campaign that keeps fraud awareness high on the public agenda and encourages customers to adopt concrete, conscious behaviours that reduce their exposure to fraud. The sector will continue to invest in this area in order to make consumers more resilient and thus avoid fraud. It is important that the government (by analogy with the BOB campaigns) and other stakeholders support and facilitate these campaigns. Such a coordinated approach can create a strong leverage effect, further strengthen fraud prevention and enhance citizens' resilience.

Conclusion

Online fraud has become a structural and evolving societal challenge that can no longer be addressed through isolated measures or by a single group of actors. **The banking sector fully recognises its responsibility and has already taken, and continues to take, far-reaching initiatives to strengthen customer protection, enhance fraud detection and support victims**. Through this action plan, banks commit to further reinforcing their efforts at both individual and sector level, including additional operational safeguards, strengthened cooperation and increased customer awareness.

At the same time, this action plan clearly demonstrates that banking measures alone are not sufficient to deliver a sustainable reduction in online fraud. Even the most robust bank-level and interbank initiatives will only mitigate part of the problem if fraud continues to originate and evolve elsewhere in the chain. **A lasting impact requires a fully coordinated ecosystem approach, in which all relevant public and private actors assume their responsibilities** and act in a coherent and complementary manner.

Banks are prepared to do more and to continue investing in prevention, detection and customer protection. However, these efforts can only be effective if they are matched by decisive action upstream and downstream in the fraud chain — including by online platforms, telecom operators, law enforcement authorities and public bodies. Without such alignment, there is a real risk of displacement effects, whereby fraud shifts towards the weakest link. **Avoiding such fragmentation is essential to ensure that Belgium does not become an attractive target for organised online fraud.**

This action plan therefore calls for strong political support, clear coordination and an enabling legal framework that allows innovation, information sharing and effective enforcement, while fully respecting fundamental rights. Only through a shared, balanced and integrated approach can online fraud be tackled at its source, customer protection be strengthened in a sustainable way, and trust in the digital financial ecosystem be preserved.

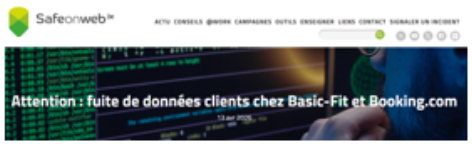
Attachment: example of fraud journey

Banks are mostly involved down the journey - during and after the transaction- while phishing is generally initiated through social media and fake websites

Fraud Journey – **Phishing**

PREPARE – Data leakage

- A hotel booking platform is hacked and hundred thousands of clients' data (incl. Name, address, phone number, birth date and banking data and reservations details) are available on the dark web



PREPARE – Scenario design and impersonation

- Thanks to data collected on the dark web, the fraudster identifies potential victims' banks and designs tailored scenario (i.e., social engineering) to impersonate client's bank.

EXECUTION – Approach & Convince

- Victim receives phone call from the fraudster impersonating his bank and asking him to confirm his credentials as he might have been victim of fraud
- Because of social engineering the victim thinks that he is talking to his banker and provide his credentials
- The fraudster uses the credentials to access client's accounts

COMPLETION – Transfer & cash out

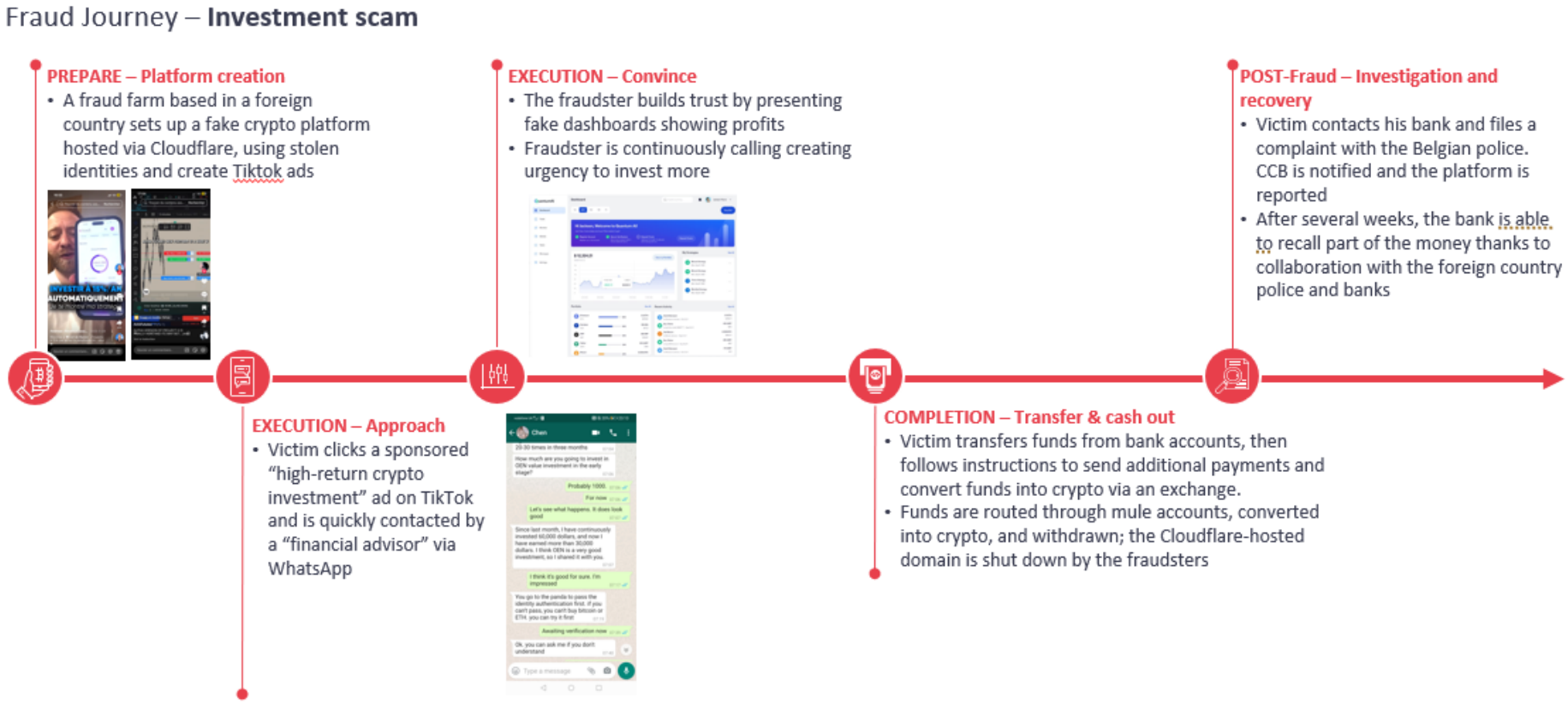
- Fraudster accesses the account, increases limits, and triggers a high-value transfer disguised as a "security test"
- Funds are sent to mule accounts, split, and partly converted into crypto or withdrawn
- The fake website and domain are quickly shut down

POST-Fraud – Investigation and recovery

- Victim detects anomaly, alerts bank, CCB (safeonweb), and police; bank traces funds and initiates takedown actions
- Partial funds are recovered; remaining losses assessed

Attachment: example of fraud journey

Investment scams are inherently facilitated by social media and telco channels which acts as echo chambers, while banks intervene only at the transaction stage[4][5]



[4] "Dans la jungle des néobanques: Arnaques, trafics et clients lésés" – Arte
[5] Newspaper clip from BBC