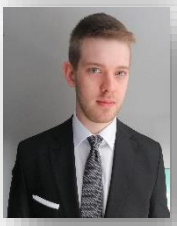
Belgian Financial Forum

Financial Market Infrastructures and Payment Services Report 2023

Jan Vermeulen
Head Payments, oversight & supervision
National Bank of Belgium

Dorien De Beuckeleer
Financial Risk Analist
National Bank of Belgium



Cédric Collaert
Analist
National Bank of Belgium

Yvanna Vieira De Melo
IT Supervisor
National Bank of Belgium

Florian Christiaens
Digital Euro Expert
National Bank of Belgium

ABSTRACT

The National Bank of Belgium (NBB) publishes yearly a Financial Market Infrastructures (FMIs) and Payment Services Report which provides for the preceding year a detailed overview of changes in the regulatory framework for FMIs, custodians, payment service providers and critical services providers, the evolution of their activities and the Bank's approaches to oversight and prudential supervision.

A number of significant FMIs (SWIFT, Euroclear, Bank of New York Mellon, Mastercard, Worldline) with international relevance are vested in Belgium and the report establishes transparency by clearly defining, and disclosing the regulatory, supervisory, and oversight policies with respect to these systems and institutions.

Also trends with regards to national payment systems and services are depicted and the annexes provide statistical time series on the FMI activities and the payments eco system. This year's publication incorporates a few topics deserving specific attention which are summarized in this article: the impact of the Russian invasion of Ukraine, the digital euro project, climate risk and cyber & IT risks.

The Russian invasion of Ukraine

The Russian Federation's invasion of Ukraine in February 2022 has had profound and cascading effects on geopolitical relations and the global economy. One of the measures taken in consequence was the announcement of the European Commission of various sanctions packages targeting entities in or affiliated with Russia or Belarus. Those sanctions, as well as the Russian countermeasures, had an impact on some of the institutions that are subject to the National Bank of Belgium's oversight and supervision.

The impact of Russian sanctions and countermeasures adopted by Russia on Euroclear Bank remained an important attention point for the Bank in its supervisory activities. Blocked securities positions due to sanctions still generate income and redemption payments impacting the size of Euroclear Bank's balance sheet significantly. On the other hand, Russian countermeasures affect holdings of Euroclear Bank on behalf of its participants with a Russian nexus.

The Russia-Ukraine conflict also affects BNYM SA/NV. Given its specific business model, BNYM SA/NV had to take care of correctly implementing sanctions that were common to every bank and financial intermediary (albeit due to its global presence BNYM SA/NV has to implement different sets of sanctions) but also specific attention points relating to activities like Depository Receipts (DR's) etc.

Included in the various EU sanctions packages is the prohibition to provide specialised financial messaging services to the banks specifically listed in the sanctions decisions. In order to remain compliant with European laws and regulations, Swift had to disconnect 10 Russian and 4 Belarusian banks from the financial messaging network.

In order to be continuously in compliance with European laws and regulations, Swift is expected to keep track of changes in the ownership structures of its users, as any legal person, entity or body established in Russia or Belarus whose proprietary rights are directly or indirectly owned for more than 50% by a sanctioned entity will also become a sanctioned entity by operation of law and should be disconnected from Swift's financial messaging network accordingly.

Swift FIN traffic growth in 2022 was slightly lower than in previous years, in particular for payments. One of the explaining factors is the traffic lost because of the disconnection of sanctioned banks, next to the reduced interactions with Russia and Belarus triggered by sanctions overall. Year-end figures for 2022 show that Swift FIN traffic sent to/received from Russia decreased by 55% and 60% respectively; for traffic sent to/received from Belarus, the decrease measures 62% and 70% respectively. This traffic decrease only kicked in as of March/April 2022, following the Russian invasion of Ukraine and the ensuing establishment of sanctions.

The digital euro project

The National Bank of Belgium, in collaboration with the European Central Bank (hereafter 'the ECB'), is pursuing the preliminary work for the potential introduction of a digital euro, the main objectives of which would be to further stimulate the digitalisation and efficiency of the European economy

while strengthening the strategic autonomy of the euro area without competing with private payment solutions. The Eurosystem is thus currently working on the investigation phase, which started in October 2021 and will last until September 2023. During this phase, the Eurosystem will seek consensus on technical questions and study the implications of the issuance of a digital currency on payment infrastructures, financial stability and financial inclusion.

As a reminder, consultation rounds and focus groups have been held with citizens of the euro area throughout 2020 and 2021 . Moreover, a regular dialogue on a digital euro has been established with all market participants , including banks, other payment service providers, consumer representatives and merchants through the Market Advisory Group (hereafter 'the MAG') or the Euro Retail Payments Board (hereafter 'the ERPB') at European level and the National Retail Payments Committee (hereafter 'the NRPC') at the Belgian level. The national central banks are also deeply involved in the investigation process, both through participation in the High-Level Task Force (hereafter 'the HLTF - CBDC') and the Project Steering Group (hereafter 'the PSG'). The HLTF is responsible for taking major decisions on the functionality and intrinsic characteristics of the digital euro, whereas the PSG coordinates the study and research efforts of both national central banks and the ECB. The joint work of both, linked to the insights gained from the consultations and the various focus groups, has thus allowed progress to be made in the design of a potential digital euro.

Among the decisions taken so far, one of the main ones concerns the "transfer mechanism", i.e., the procedure by which transactions and their validation are carried out. As such, the Eurosystem has approved the further exploration of an "online third-party validated solution" and an "offline peer-to-peer validated solution". The first (online validated transaction by a trusted authority) is similar to transfers via commercial banks while the second one is similar to transactions performed between two individuals using their smartphone (or other devices) without being in an online internet modus (i.e., similar to a cash transaction). However, the time to market for the latter solution is more uncertain due to its reliance on NFC or similar hardware-based technologies. The development of the first "online third-party validated solution" will not be delayed if the timely delivery of a validated peer-to-peer solution for offline payments proves unfeasible.

In addition, regarding the settlement model and the role of intermediaries, it was decided that transactions would be settled at the Eurosystem level for online transactions and at the local storage device level for offline transactions. Transaction management tasks would be carried out by supervised intermediaries (credit institutions or payment service providers), who would be the direct contact entities for private individuals, merchants and companies using digital euro in their role of depositories of the contractual account management relationship with the end user.

Another crucial feature of the digital euro according to the public is privacy and it has also been the subject of thorough reflections over the past few months. While initially, in a baseline scenario, it was considered to mirror current AML/CFT practices of private sector digital solutions, it was decided that the Eurosystem would explore two additional options, diverging from these practices in favour of more privacy (while not impeding the appropriate exercise of AML/CFT controls). These options are (i) selective confidentiality for low-value online payments and (ii) an offline functionality which ensures that the users' balances and transaction data remain private. Further work is still needed to

explore how both options could be activated, either under the current regulatory AML/CFT framework or under a new tailored regime. In addition, various privacy-enhancing technologies are being tested for the online solution.

Finally, a significant step toward financial stability taken recently is the exploration of tools to control the potential amount of digital euros in circulation. Indeed, if held by users in large volumes, a digital euro could lead to a structural substitution of commercial bank deposits, which could have an adverse impact on monetary policy, financial stability and credit flow within the real economy. To quote Marcus Brunnermeier: “the digital euro should be present everywhere but important nowhere, should be successful but not too successful" . As such, several mechanisms to prevent the rise of such adverse effects were discussed. These include e.g. quantitative limits and remuneration-based tools. The former is able to limit the individual use and speed of conversion of deposits while the latter could reduce the attractiveness of digital euro holdings beyond a certain threshold compared to other highly liquid and low-risk assets. Both tools will be included in the design of a potential digital euro so that the relevant tool and settings thereof can be defined closer to the time of issuance. Which will then give the opportunity for the Eurosystem to consider the actual economic, financial and monetary policy environment (e.g., interest rates, the level of excess reserves, etc.) and keep the necessary flexibility in the future. In addition, the Governing Council agreed on the possibility of using a so-called "waterfall" functionality, whereby funds in the digital euro wallet exceeding the holding limit would be automatically transferred to a linked commercial bank account. The inverse functionality (namely "reverse waterfall") will ensure that end-users can make a payment even if the amount exceeds their current digital euro funds, by taking additional liquidity from the user's linked commercial bank account. Both features, activated at the discretion of the end-user, will ensure a seamless payment experience, thereby preventing the holding limit from becoming a transaction limit.

On top of the above-described decisions in relation to the design of a potential digital euro, in-depth work is also taking place, in relation to the development of a prototype for a digital euro (centralized back-end infrastructure) and the collaboration with selected market players for the construction and design of several user interface prototypes (front end infrastructure) according to the wide range of usage scenarios for which the digital euro will be usable, e.g., peer-to-peer online transactions (CaixaBank), peer-to-peer offline transactions (Worldline), e-commerce transactions (Amazon), point-of-sale payments in physical shops (initiated by the payer - EPI ; initiated by the payee - Nexi). It should be noted that transfers to governments and from governments are also part of the list of use cases prioritized by the ECB. However, no front-end infrastructure prototype is currently being studied or tested for such use cases.

The user interface prototype development exercise serves as a learning exercise, results thereof are expected in the first semester of 2023 and will be published). There are no plans to re-use the prototypes in later phases (e.g., realisation) of the Digital Euro project.

Furthermore, the ECB is also working on a draft of a digital euro scheme rulebook, i.e., a set of rules for payment transactions with a digital euro. This approach is considered to be the most efficient way to achieve the objectives of a digital euro and to capitalise on the respective strengths of the public

and private sectors. Indeed, a specific scheme would establish a set of common rules, standards and procedures that would ensure pan-euro area reach and promote a harmonised end user payment experience, as certain requirements on commercial elements could be specified and give significant flexibility to respond to end user preferences and specificities. A scheme rulebook manager was appointed at the beginning of December 2022 (Mr. Christian Schäfer) to set up and coordinate the Rulebook Development Group, composed of representatives of the Eurosystem national central banks and market participants (including consumer delegates).

Finally, in parallel with this Report, the Eurosystem continues to actively engage with all stakeholders, with new round of focus groups planned around prototype completion during the remainder of the investigation phase. The Eurosystem will decide in autumn 2023 whether to proceed to the preparation phase. Meanwhile, the European Commission aims to provide the legislative groundwork necessary to implement a digital euro in the second quarter of 2023.

Environmental and climate-related risks within the FMI landscape

Climate and environmental risks are becoming increasingly important and are also gaining attention in the financial sector. Multiple general and international frameworks have been published with the aim to tackle climate issues and to mitigate greenwashing. Specific guidance (ECB/EBA/NBB circular) were published for banks, based on a translation of these international guidance. However, there is no dedicated and aggregated set of requirements and/or guidance for CSDs, payment transactions processors and messaging services.

The NBB has decided to not only follow up on climate and environmental risks for banks and insurance companies, but to extent the analysis on its own initiative to CSDs, payment transactions processors and messaging services considering opportunities as well as direct and indirect impacts. The NBB decided to pay attention to these institutions as they play a central role in supporting the financial sector. Hence, the Bank requested end 2021/beginning 2022 a sample of Belgian institutions active in this area to complete a questionnaire on climate and environmental risks. The first insights gained from this questionnaire were presented in the 2022 NBB Financial Market Infrastructures report. The NBB will continue to interact with market infrastructures and payment institutions and perform analyses with regards to climate and environmental risks on a structural way. This will include a mix of firm-specific and horizontal analysis based on different forms of interaction (questionnaires, meetings, …). The firm-specific analysis can point out the strengths and weaknesses, opportunities and treats, as well as the progress made at the level of the institution. The outcome of the horizontal reviews includes amongst others describing the general trends and evolutions observed (e.g. the climate and environmental domains in which was made the most progress and which domains are still in the early development stage) within the FMI landscape, custody banks, payment transactions processors and messaging services landscape as well as highlighting similarities and differences noticed between different institutions. More broadly, such analyses can give an indication, for each of the different climate and environmental domains which institutions are showing the most progress and which institutions are lagging behind on the different dimensions of the framework in

comparison with their peers, hence giving a robust base for benchmarking and level-playing field setting.

The follow-up will consist out of a mix of global reviews as well as in-depth analysis of selected domains impacted by climate and environmental related risks and opportunities. Some of the institutions targeted in this presentation and having also a banking license are already requested to comply with several of these guidelines in the framework of the banking supervision. The NBB approach to climate and environmental risks encompasses the entire FMI, custodian and payment transactions processors and messaging services landscape whatever their status and related set of applicable guidelines is, as well as their relative maturity and implementation timeline. The follow-up of climate risks will include different domains, like:

- *Materiality and business model*: assessment of the materiality of climate and environmental risks in the short, medium and long term to ensure the sustainability as well as the resilience of the business model.
- *Governance*: awareness, expertise present and specific responsibilities within the different layers of the organisation.
- *Risk appetite and management*: existence of processes to identify, measure, mitigate and report about climate and environmental risks throughout the different layers of the institution.
- *Disclosures*: publication of sufficiently detailed and accurate, non-confidential information to the public.

Market infrastructures and payment institutions can play a role in the financial community with regard to tackling environmental and climate-related risks. The participants of these institutions are also confronted with changing needs and new challenges due to climate risks. These institutions can support their participants by offering solutions helping their participants to tackle climate and environmental risks. On the one hand, the institutions are developing climate and environmental related solutions supporting clients' needs. To achieve this, the institution can offer new products/services as well as integrate ESG components into the existing products and service offering.
Some examples:

- Swift: has integrated the International Chamber of Commerce's Sustainable Trade Finance Guidelines into their Know Your Customer Registry platform. A platform where clients can register their own Know Your Customer Data and have access to their counterparties' Know Your Customer Data.
- CSDs/custodians (such as BNYM): possibility to add ESG factors to the collateral eligibility scheme negotiated between their clients in the collateral management and securities lending business
- Issuance, safekeeping and administration of green bonds.

On the other hand, in order to offer these new or extended services, the institutions could also engage into strategic partnerships, often with specialized firms. To give an example, Euroclear

engaged in a partnership with Greenomy, an institution which helps companies to comply with new EU sustainable finance legislation by digitalizing the data capturing & reporting process and providing data analytics features.

Beside greening the economy, financial market infrastructures must manage their own climate-related threats and challenges in order to be able to ensure the continuity of operations that is crucial to the functioning of the financial markets. It is important that these institutions determine what their challenges are and define how they will deal with these challenges and which mitigating measures they must take in this regard.

CSDs, custody banks, payment transactions processors and messaging services are all highly operation-driven institutions. They are offering safekeeping of assets in electronic/dematerialized form and/or having highly transaction-driven businesses, often with a high level of automation. Consequently, they are heavily relying on IT and digital services. This implies that climate and environmental risk drivers are mainly situated at the level of the operational risks and business continuity.

As these institutions are highly reliant on IT and digital services, the availability of their IT and data services at any moment in time is of high importance to guarantee the continuation and quality of their operations. As the institutions in scope of this presentation are playing a central and often international role in the financial sector, a service disruption can seriously disturb the functioning of the (international) financial markets. This was also confirmed in the first stocktake exercise, where these institutions identified physical risks; like floods, storms, earthquakes and rising temperatures as an important risk category for their institutions, as these risks can impact the services offered by the institutions themselves or affect them indirectly when their service providers are hit by such types of event. Consequently, these institutions should identify how the different climate elements can impact their IT and data centres and take sufficient protection and back-up measures to protect these operating/IT/data centres against the impact of increased frequency of extreme weather events and natural disasters. Moreover, this is complexified by the global presence of several market infrastructures and/or payment institutions implying several operational centres located in different continents/areas which entails specific forms of climate-related risks. These institutions will be confronted with a broader set of extreme weather events or natural disasters as different locations bring different risks; e.g. certain locations are more hit by floods, other by extreme heats or earthquakes; each bringing its own challenges and mitigating measures.

Besides the physical risks, the institutions listed also several transition risk drivers, like energy-related elements which bring additional challenges. Emission norms and energy costs are increasing, in a context where energy use could be higher due to rising temperatures leading to higher cooling needs of IT/data centres. Moreover, the institutions often rely heavily on digital services, automation, data driven services and the use of artificial intelligence which could be energy-consuming; whereas the

need for reduction of (fossil) energy consumption and being energy-efficient is increasing and even requested by different stakeholders (clients, imposed by regulation,…).

Climate risks could also have an indirect impact on custodians and CSDs profitability. The custody fees are partially billed on the basis of the value of the assets under custody. Securities which are held in custody at the CSD or the custodian and which are issued by companies active in "brown" industries or located in areas more exposed to climate and environmental risks could tumble and might consequently erode the collected custody fees.

Cyber and IT risks

Digital operational resilience

Digital operational resilience was one of the Bank's top priorities again in 2022. The Bank is not the only regulator focusing on this risk. In this context, the Bank's staff actively contribute to various policy initiatives. In March 2021, the Basel Committee on Banking Supervision published new principles for strengthening the operational resilience of banks, including a specific focus on ICT and cyber security. At EU level, the Digital Operational Resilience Act (DORA) entered into force on 17 January 2023 and its provisions shall apply as of 17 January 2025. They aim at mitigating the risks associated with the digital transformation of the financial industry by imposing strict common rules. These rules apply to a wide range of financial institutions, plus critical IT third-party service providers, for example cloud service providers, who would be subject to a form of EU oversight.

The initiative for this Act was taken by the European Commission's directorate-general for Financial Stability, Financial Services and Capital Markets Union (DG FISMA) in response to the 2019 Joint technical advice of the European Supervisory Authorities (ESAs) that called for a more coherent approach in addressing ICT risk in finance[1] and as part of a much broader Digital Financial Strategy setting out general directions on how the European Union intends to support the digital transformation of finance in the coming years, while regulating and mitigating the risks arising from it.

The DORA regulation is motivated by the ever-increasing dependency of the financial sector on digital assets and processes, resulting in information & communication technology (ICT) risks posing a challenge to the operational resilience, performance and stability of the EU financial system as a whole. The Commission made the proposal on the ground that current legislation across member states does not fully address the topic in a detailed and comprehensive way, does not provide financial supervisors with the most adequate tools to fulfil their mandates, and leaves too much room for diverging approaches across the Single Market.

1 Joint Advice of the European Supervisory Authorities to the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector, JC 2019 26 (2019)

The DORA proposal contains five distinct pillars:

- **Governance** and **ICT risk management** related key principles and requirements for financial entities, inspired by relevant international, national and industry-set standards, guidelines and recommendations. These requirements revolve around specific functions in ICT risk management (identification, protection & prevention, detection, response & recovery, learning & evolving, and communication), but also underline the importance of an adequate governance and organisational framework. Amongst others the crucial and active role the management body has in steering the ICT risk management framework and the assignment of clear roles and responsibilities for ICT-related functions is covered by this first pillar.
- The second pillar relates to requirements for financial entities with regard to **managing** and **classifying ICT-related incidents**, and a proposal to harmonize and streamline the **reporting** of such major incidents to the competent authorities, next to responsibilities for competent authorities in providing feedback and guidance to financial entities and in forwarding relevant details to other authorities with a legitimate interest. The ambition put forward is for financial entities to have to report major incidents only to one competent authority. To this end, the feasibility of a single EU hub will be studied by the ESAs, the ECB and ENISA. In the same spirit, the incident reporting obligations under PSD2 will be fully integrated into this new incident reporting framework.
- The third pillar addresses requirements for **digital operational resilience testing**, i.e. periodically assessing cyber resilience and identification of weaknesses, deficiencies or gaps, as well as the prompt implementation of corrective measures. While all financial entities should test their ICT systems by making use of tests ranging from vulnerability scanning to software code analysis, only those entities identified by competent authorities as significant would be required to conduct advanced Threat Led Penetration Tests.
- Fourth, the proposal contains provisions to ensure the sound management of **ICT third-party risk**. On the one hand, this objective will be achieved through the respect of **principle-based rules** applying to financial entities' monitoring of this risk and through regulation that **harmonises key elements** of the service and relationship with ICT third-party providers. On the other hand, the regulation seeks to promote convergence on supervisory approaches to ICT-third-party risk in the financial sector by **subjecting critical ICT third-party service providers to a Union oversight framework.**
- The last and fifth pillar raises awareness around ICT risk and related aspects such as: minimising the propagation of risk, supporting financial entities' defensive capabilities and threat detection techniques, explicitly allowing financial entities to set up **cyber threat information and intelligence exchange** arrangements amongst themselves.

A broad range of financial entity types is in scope of DORA, amongst others central securities depositories, credit institutions, insurance and reinsurance undertakings, investment firms, payment institutions and electronic money institutions. By having this broad scope, DORA seeks to harmonise approaches across the financial sector with the objective of an increased operational resilience and to ensure a safer and more stable overall financial system. Operators of payment systems and entities involved in payment processing remain out-of-scope for the time being.

DORA is to be considered so-called "lex specialis" with respect to the EU Directive on measures for a high common level of cybersecurity across the Union (also referred to as the NIS 2 Directive)[2]. This means that the requirements under DORA regarding for example ICT risk management and ICT-related incident reporting are in principle more far-reaching than those under the NIS 2 Directive and that institutions in the personal scope of DORA only have to comply with the DORA provisions, unless the national transposition of NIS 2 would explicitly extend the scope or provisions of the NIS 2 Directive (and therefore deviate from the minimum harmonization principle).

The EU legislators have further specified that, given the strong interlinkages between the digital resilience and the physical resilience of financial entities, the obligations laid down in Chapters III and IV of the Directive on the resilience of critical entities (CER)[3] should not apply to financial entities falling within the scope of DORA. Here too, the national transposition of CER could still extend the scope or provisions of the CER Directive.

Overall, the Bank is very supportive of the DORA initiative, its ambition to strengthen digital operational resilience and to further harmonize ICT risk management practices and requirements in the financial sector. The Bank is fully committed to a successful implementation of DORA and is actively contributing to the establishment of level 2 texts that will support the final DORA regulation.

Threat Intelligence Based Ethical Red Teaming in Belgium (TIBER-BE)

In 2018, the Bank set up a framework for ethical hacking, namely TIBER-BE (Threat Intelligence Based Ethical Red Teaming Belgium). This program is the Belgian implementation of a methodology developed by the Eurosystem, which aims at increasing the cyber resilience of individual FMIs and financial institutions through sophisticated tests, as well as to gain important insights into the cybersecurity of the Belgian financial sector as a whole. The Bank encourages these exercises in its role as catalyst for financial stability. More information on this TIBER-BE implementation can be found in the thematic article 8 on TIBER-BE.

Since the inception of the TIBER-BE programme, the cyber-threat landscape has changed at a breakneck pace, not in the least related to the evolutions witnessed in geopolitics. Besides increased threats from organised criminal groups orchestrating cyber-campaigns in pursuit of profit through data theft and ransomware, the Russian invasion in Ukraine has sparked a major uptake in cyber activity by threat actor groups and individuals taking a side in the conflict and conducting operations in support thereof. For now, related cyber-attacks are primarily targeted towards Ukrainian and Russian IT infrastructure, but it is not unlikely for actors active in the conflict to eventually shift their focus towards targeting nations and entities outside Ukraine and Russia using their newly acquired techniques. This increased threat looming from the east has led Western financial entities and critical

2 Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (14 December 2022)

3 Directive (EU) 2022/2557 of the European Parliament and of the Council on the resilience of critical entities and repealing Council Directive 2008/114/EC (14 December 2022)

infrastructure alike to increase their level of preparedness for potential cyber-attacks. In the effort of verifying whether a sufficient level of cyber-resilience is achieved and strengthening the defensive measures where needed, the TIBER-BE programme has proven to be a valuable tool. Through the treat-intelligence-based scenarios making up a TIBER-BE engagement, actual and relevant threat actors and the techniques they use are emulated. This enables the tested entities to identify and remediate weaknesses that are most likely to be targeted and exploited by these selected threat actors.

After 3 years of TIBER testing, all entities in the initial scope of the programme have been subjected to a TIBER-BE engagement. While setting up such a new initiative might be challenging, all tests performed so far can be deemed successful, with a number of lessons learnt for all entities involved. The success of this first cycle helped establishing the framework's reputation and clears the way for subsequent rounds of TIBER-BE testing. The increased credibility brought by the successful first round of TIBER-BE engagements allowed the programme to grow both in size and thoroughness of the testing approach. For the second round of testing, several new entities have been added to the scope of the programme. This extension consequently improved the coverage of TIBER testing, further bolstering the programme's ability to enhance the cyber resilience of the Belgian and European financial system. Additionally, for the entities that already underwent a TIBER-BE engagement, the experiences from the first test have enhanced their familiarity with the TIBER framework which should lead to an increased willingness of these entities to undergo more extensive and more thorough TIBER tests in the future.