Securing Trust in Central Bank Digital Currencies

WHITE PAPER

Executive Summary

There is no doubt that the digital economy is increasingly becoming *the* economy, as consumers, businesses, and banks seek more convenient, secure, and speedy payments. Even before COVID-19, cash use has been declining as more transactions take place through digital channels.

Central banks are the linchpin of the financial system—the source of trusted money for hundreds of years. Recognizing that their economies increasingly operate in the digital realm, central banks are actively weighing the pros and cons of offering a retail central bank digital currency (CBDC) for the general public to use in day-to-day payments.* Indeed, 80 percent of central banks report that they are actively weighing the merits of a CBDC for their economies.[1] As central banks accelerate their exploration of general purpose or retail CBDCs, they will necessarily have to engage an ecosystem of participating banks, payment service providers, data service providers, payment networks, and a variety of technology resources.

A retail CBDC has the potential to support many objectives of central banks, including payments safety, efficiency, and financial inclusion. However, it is inevitable that CBDCs will also attract the attention of bad actors. The skills needed to defend a retail payment system—securing millions of endpoints against fraud, rooting complex financial crime networks, and ensuring operational resiliency in the face of sophisticated cyberattacks—are fundamentally different from those central banks employ to secure their wholesale payment systems today.

Fortunately, central banks need not reinvent the wheel. Prospective CBDCs can benefit from many of the hard-won lessons and sophisticated tools that private payment networks have developed for their retail payment systems over the past half-century.

Mastercard is committed to helping central banks explore the opportunities CBDCs present. One way we can do that is by sharing the tools and expertise needed to keep digital currencies secure—enabling central banks to protect millions of endpoints, employing artificial intelligence (AI) to detect financial crime, and gathering cyber-risk signals from every corner of the globe.

Mastercard is also committed to building a digital economy that works for everyone, everywhere. Forging new paths for sustainable and inclusive economic growth improves the quality of life and the financial security of all segments of society. We share central banks' goal to ensure the public trust in the global financial system as we help transform it to better serve the world's people.

* This paper focuses on 'general purpose' or retail CBDCs offered to the public. Any use of the term CBDC in this document refers to a retail instrument.

The world of payments is digitizing, and central banks are no exception

Central banks are carefully considering the feasibility of retail digital currencies as they continually strive to strengthen and grow their economies with greater innovation, efficiency, and security. But CBDC design and issuance are not decisions to be taken lightly. Agustín Carstens, General Manager of the Bank for International Settlements, has likened the creation of a CBDC to conducting surgery on the backbone of a country's financial system.[2]

"The monetary system is the backbone of the financial system. Before we open up the patient for major surgery, we need to understand the full consequences of what we're doing."

Agustín Carstens, General Manager, Bank for International Settlements

Over the past eighteen months, central banks around the world have rapidly accelerated their exploration of retail CBDCs: conducting in-depth economic analysis, technical proofs-of-concept, and even large-scale pilots to understand the role that a CBDC could play in achieving their economic and policy objectives. These efforts have examined everything from the unintended challenges a retail CBDC could create for monetary policy and financial stability, to the possible synergies between a retail CBDC and a modern digital identity system (the subject of a forthcoming Mastercard paper). Equally important, but less often explored, is the challenge of safeguarding a retail CBDC system from external threats.

Trust and security sit at the heart of payments. Users must know that the system will be accessible and operational where and when it is needed; that their funds, accounts, identity, data, and privacy are secure; and that they will be protected in the event of fraud. Central banks recognize this security challenge—the European Central Bank recently noted that a digital Euro "will need to be highly resilient to cyber threats and capable of providing a high level of protection to the financial ecosystem from cyberattacks"[3]—but there has been little discussion of the true size of the challenge. A retail CBDC will inevitably face sophisticated attacks from both private and state-sponsored actors. But central bank's long experience safeguarding their wholesale payment systems will provide few of the tools and experience needed to secure the radically different topology of modern retail payment systems. Deploying a retail CBDC will require a central bank to combat threats at an unprecedented scale and speed. Among the many strategies needed to secure their ecosystem are these:

1. Secure millions of endpoints connecting consumers, banks, Fintechs, businesses, and other players that form a nearly infinite web of digital connections
2. Provide supervised intermediaries a network-level, 30,000-foot view of the financial ecosystem to better anticipate fraud, money-laundering, and other financial crimes
3. Monitor global risk signals in real time so that all ecosystem players can rapidly defend against fraud

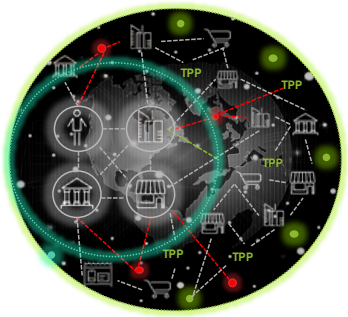
Fortunately, central banks considering a retail CBDC need not reinvent the wheel to achieve security. Existing retail payments providers, like Mastercard, have decades of experience addressing these kinds of security challenges on B2B2C networks that strongly resemble the two-tier CBDC

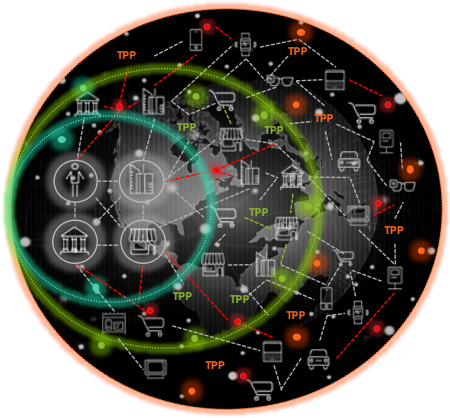
architectures being envisioned by most central banks. We are eager to share that experience, and the tools we have built, with central banks. In this paper, we will share our outlook on some of the biggest challenges a retail CBDC might encounter and consider how central banks could leverage a mix of private-sector learnings and capabilities to efficiently and effectively address these issues.

Challenge 1 – Infinite endpoints

Retail payment systems have many more endpoints than the wholesale payment systems most central banks are familiar with. And as innovations like real-time payments, the Internet of Things (IoT), 5G mobile networks, and CBDCs bring even greater convenience and speed to our financial system, each point of interaction is also another opening for thieves. Modern retail payments networks—permeated by a much larger number of undefined connections as consumers use more devices, apps, and channels—are inundated by a torrent of payment flows that must be protected. It is no surprise that these emerging digital channels have become fertile breeding grounds for criminals, and fraud and financial crime have grown exponentially.

As the payments ecosystem evolves, we must safeguard the trust consumers have long expected





Early Ecosystem

- Well-defined stakeholders with protected connections
- Mostly in-person purchases
- Few large-scale cyber-threats

Current Ecosystem

- Growing acceptance of digital payments
- A mix of in-person and digital commerce
- Payment credentials stored in numerous physical and digital locations
- Cyber-threats of increasing scale and sophistication

Future Ecosystem

- Exponential growth of IOT with each device serving as a payment endpoint
- Digital-first is the default behavior
- Highly sophisticated cyber-threats enabled by advanced AI tools

Lessons Learned: Building tools to assess third-party cyber risk

As more people get connected with more of their devices, the resultant impact is that organizations need to constantly monitor the cyber environment of all online presences in order to identify cyber risks and vulnerabilities before they can be exploited. Mastercard has long understood that it is not enough to prevent fraud at the payment transaction, that we needed to widen the net and stop fraud upstream. We have broadened our focus from transaction to interaction. Today, we have moved wider still by introducing new tools that enable online environments to proactively manage and maintain their security. You might think of this as the security checks a traveler encounters before they board a plane to fly somewhere: our cyber tools and capabilities are the safeguards that ensure that the plane is safe to fly, all systems have been checked and tested, and it is fueled before it takes to the air.

One of the many tools we use to secure the Mastercard network is RiskRecon.™ This service helps organizations—including issuers, acquirers, and merchants—proactively monitor, identify, and remediate security and cyber risks across their supply chain by automating cyber risk assessments and by continuously monitoring third parties across numerous security domains and dozens of security criteria. This helps organizations gain greater accuracy and control in evaluating and managing cyber risk from third-party relationships—ultimately enabling them to reduce financial losses and save time and resources dedicated to managing cyber threats.

RiskRecon has helped numerous organizations within Mastercard's payment ecosystem to significantly reduce their cyber risk from third-party service providers:

10% of a large U.S. FI's vendors posed a high risk	A large U.S. financial institution struggled to accurately assess risk exposure from third-party service providers critical to their business. RiskRecon performed a detailed cyber risk assessment of 1,500 providers, assessing each one's cyber environment risk along with the procedures used to combat issues that might arise. We discovered that 10%—150—were high risk.
10K+ Global FI can now readily monitor all 10,000+ service providers	A large global financial institution found it impossible to assess each of its more than 10,000 third-party service providers. Each employee on the risk management team was only able to assess a few dozen providers each year, due to its complex and largely manual monitoring process. RiskRecon automated that task to minimize manual intervention and readily monitor all 10,000+ providers.
$630K+ Fortune 500 FI now saves $630K yearly with continuous monitoring	A Fortune 500 financial institution found it difficult to identify and prioritize cyber threats from vendors—wasting spent time investigating non-critical issues while leaving critical cyber risk issues unnoticed and unresolved. RiskRecon's continuous monitoring and prioritization of vendor risk helped the financial institution reduce cyber risk by half over three years and save $630,000 annually in people, process, and technology.

With the exponential growth in digital touch points, all players struggle to defend themselves against sophisticated threats from an endless number of directions—and a CBDC will be no exception. Tools like RiskRecon could help the members of a CBDC ecosystem determine if vendors and service

providers pose a threat to their security, and what actions they should take to reduce these risks. For example, it could help financial institutions and merchants pinpoint and prioritize cyber risk by:

- Assigning a cyber risk rating for every third-party service provider and vendor based on the assessment of their cyber environment, using machine learning algorithms and verifiable data collected from public domains
- Benchmarking third-party service providers and vendors against standardized compliance frameworks and among one another
- Sending alerts when risk thresholds are triggered, recommending actions to reduce third-party risks, and providing risk plans that can easily be shared with vendors

With the exponential growth in digital touch points, all players struggle to defend themselves against sophisticated threats from an endless number of directions. Central banks that work with the private sector to monitor every endpoint in their CBDC's ecosystem—identifying cyber-vulnerabilities before they become an issue—will be best positioned to deliver a retail payment experience that meets their citizens' expectations for trust and security.

Challenge 2 – Viewing risk across the ecosystem is critical to managing its potential impact on your enterprise

While supervised intermediaries in a two-tier retail CBDC ecosystem will likely be responsible for conducting their own KYC and AML activities, their inability to track transactions beyond their four walls leaves them vulnerable to financial criminals—who have developed sophisticated tools that exploit such limitations. At the same time, the speed and instantaneous finality envisioned for real-time CBDC transfers will strain the ability of many existing anti-money laundering processes to accurately identify and flag suspicious transactions in real time. Indeed, criminals are already exploiting existing real-time payment systems by rapidly moving the proceeds of crime between accounts, making it difficult for financial institutions to identify, track, and recover illicit funds. To avoid inadvertently facilitating financial crime, central banks that issue CBDCs must do more than set stringent KYC and AML standards for supervised intermediaries. Central banks must provide a network-level view that empowers all intermediaries to more effectively identify and trace financial crime as it moves across the ecosystem.

Lessons Learned: Trace Financial Crime demonstrates the value of a network view

One of the first and most successful faster payments networks is The UK Faster Payments Service, which runs on Mastercard Vocalink's real-time payments infrastructure, enabling consumers and businesses to make immediate payments 24x7, 365 days a year. By integrating network-level data from a consortium of participants in the UK faster payments network and Pay.UK , and then overlaying cutting-edge analytical techniques, we were able to significantly improve the detection and mapping of stolen funds to match the criminals' real-time exploitation.

We brought together two years' worth of Faster Payments transaction data in order to build a model of the UK's payments network, connecting over 100 million accounts across FIs that in turn linked over 375 million individual payment account relationships. Within just a few weeks of our launch in October 2018:

100M+
accounts were examined to uncover multiple money laundering rings and 100s of mule accounts

- Thousands of UK accounts were subject to further investigation due to suspicious activity, a significant percentage of which were subsequently identified as mules
- Multiple, large, well-concealed money laundering rings were uncovered where money was being moved between networks of accounts and institutions
- Hundreds of mule accounts that were completely unknown to financial institutions were identified

A network-level view of financial crime

Financial institution view

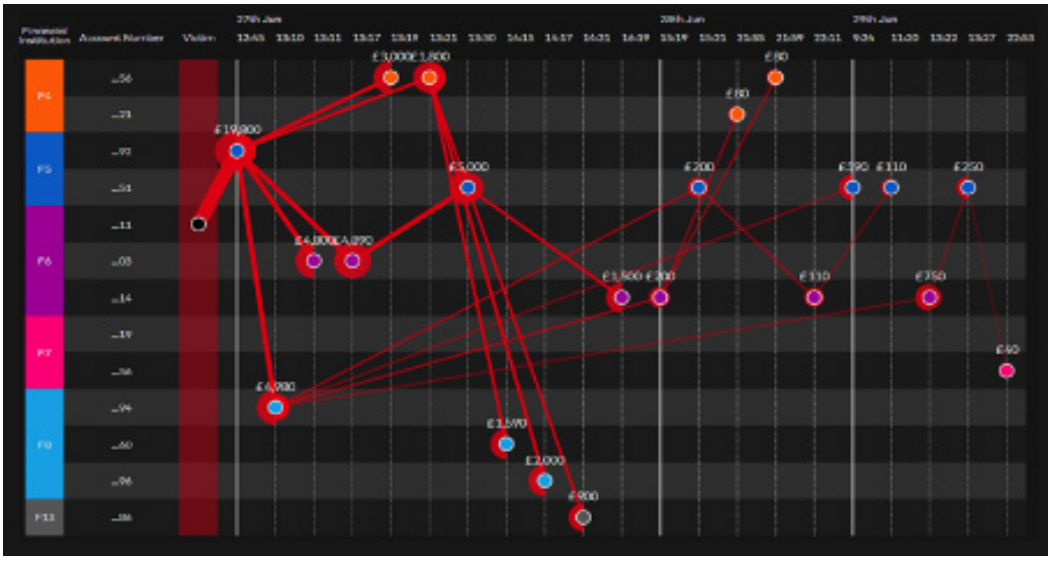
First movement of illicit funds

A bank's view of money laundering is limited to the movement of illicit funds within its own accounts. Once the funds leave the financial institution's accounts, it loses sight of them.

Network view

Subsequent movements of illicit funds

Money launderers quickly move illicit funds between accounts across multiple financial institutions. The further away they move, the lower the chance of tracing or repatriating illicit funds.



Since then, many thousands more mule accounts with hundreds of millions of British pounds in funds related to mule activity have been identified and closed using our service, which is 85X more accurate than traditional alerts on mule activity.

A central bank developing a CBDC will need to consider developing—or acquiring—a similar set of capabilities. Doing so will support the identification of criminal networks, the repatriation of stolen funds, and create a step change in the fight against organized crime and terrorism. Mastercard would be delighted to share operational and technical lessons learned from the development of our Trace Financial Crime solution, and to explore opportunities to collaborate with central banks on building a similar set of capabilities for a planned CBDC.

Challenge 3 – Assembling a global view of the threat-landscape

Unfortunately, even a network-level view isn't sufficient where highly skilled criminals transcend national boundaries to launch large-scale attacks from a great distance.

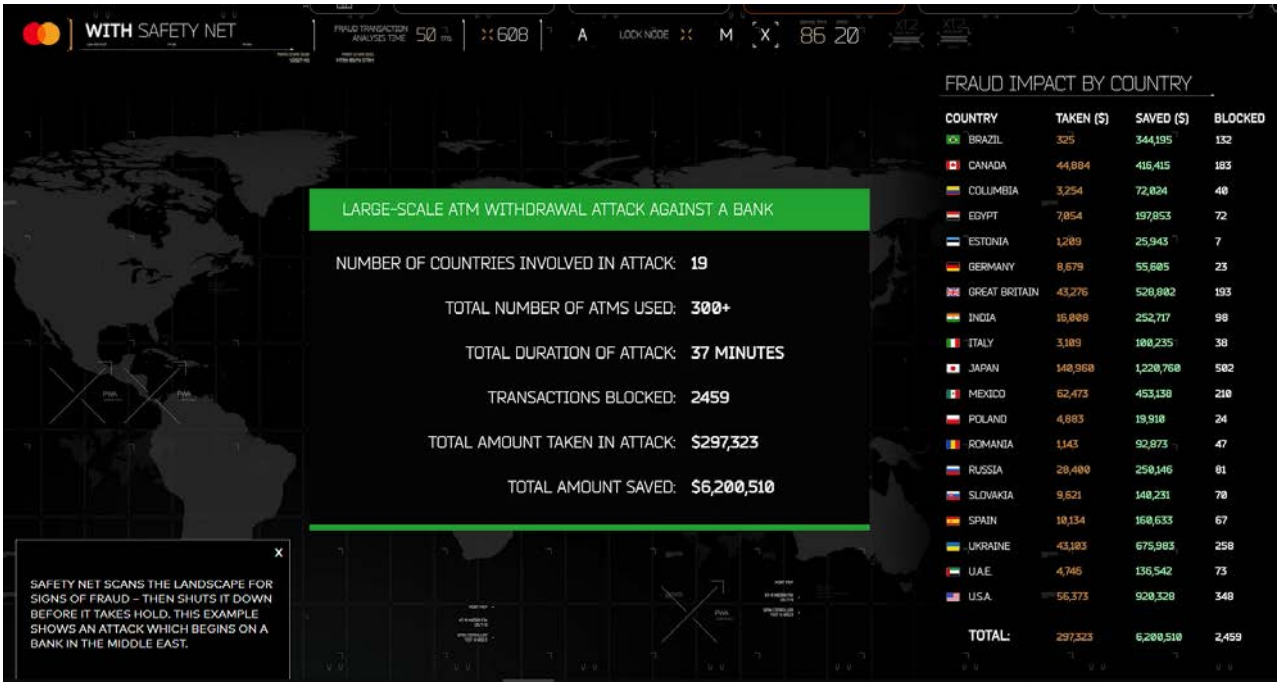
Recent years have seen a significant increase in the frequency and sophistication of cyberattacks, particularly amid the rapid digitization driven by the COVID-19 pandemic that has accelerated the adoption of digital technologies by several years. The cost to the global economy of cybercrime is expected to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025.[4] Malicious and criminal attacks are the leading cause of data breaches and the financial services sector suffers the second-highest cost per breached record, behind healthcare, with an average cost of $210 per record.[5] Unaddressed, cybersecurity concerns can hinder innovation, jeopardize trust in digital services, and even undermine national security.

While many financial service providers and institutions may think they have the tools and policies to prevent these attacks, fraudsters are proving to be exceedingly sophisticated—often covertly disabling the internal monitoring systems of their targets before launching highly coordinated attacks. These modern cybercriminals exploit both organizational silos and national borders to undermine the safety and security of critical systems.

The result is a world where no organization pursuing a strategy of cybersecurity "self-reliance," regardless of their sophistication, can be confident that their systems are secure. The safest organizations will be those that "travel together"—sharing critical insights in real time from a network that is global in scope.

To fully secure a retail CBDC from both foreign and domestic threats, central banks will need to deploy ecosystem-level monitoring tools that are global in scope; relying on partners to provide critical signals data from beyond their own borders.

Safety Net's advanced intelligence assesses the risk of large-scale attacks from over 200 million transactions a day



Lessons learned: Mastercard Safety Net® gathers global intelligence in real time

$10.7B

Safety Net declined $10.7 billion in fraudulent authorization attempts on the Mastercard network in 2020 alone

To address this challenge within our own network, Mastercard developed Safety Net. Using automated and supervised AI, Safety Net responds more quickly than human-dependent processes, providing members of our ecosystem with a secondary layer of defense that is independent from their internal systems and informed by cyber-risk signals from around the globe. With real-time visibility into large-scale global fraud events, Safety Net limits the exposure and impact of these attacks on financial institutions in our ecosystem, while helping to minimize their financial and reputational impact to the ecosystem. Safety Net declined $10.7 billion in fraudulent authorization attempts on the Mastercard network in 2020 alone.[6]

Central banks need to have a vested interest in providing supervised intermediaries in the CBDC scheme with a second line of defense that complements the day-to-day fraud safeguards of individual institutions. Moreover, the domestic scope of a CBDC means that central banks will struggle to obtain a global view of evolving cyber risks, making the CBDC an appealing target for sophisticated cybercriminals seeking to prey on that blind spot. In light of the intention of central banks representing a fifth of the world's population to issue digital currencies very soon,[2] sourcing global cyber-risk insights from the private sector will be critical to safeguarding the CBDC and its users.

It is for just this reason that Mastercard has been providing central banks, governments, and domestic payments switches with the ability to connect to the Safety Net system since 2019.

This service enables central bank networks to monitor fraud for any market around the world—providing unparalleled visibility into global fraud trends. These insights, combined with machine-learning monitoring tools, allow central banks to screen their ecosystem participants for suspicious transactions that may indicate compromised security systems. As central banks clarify the operating models and technical underpinnings of their planned CBDCs, Mastercard Safety Net could provide a second line of defense for central banks, independent of the safeguards employed by supervised intermediaries. In doing so, we hope to help CBDCs achieve the security of "travelling together" by benefiting from the insights of payment networks from around the world.

Bringing it all together – A connected approach to securing a CBDC

Central banks already have many of the skills needed to combat the cyber risks that CBDCs will face. But there are others—like securing millions of endpoints, leveraging a network-level view to stop real-time fraud, and gathering cyber-risk signals on a global scale—that many central banks will need to build or acquire. The good news is that central banks need not reinvent the wheel. To help central banks evaluate CBDC use cases, Mastercard has developed a proprietary virtual testing environment. The platform enables central banks to simulate issuance, distribution, and exchange of CBDCs between banks, financial service providers, and consumers. Critically, this testing platform provides a suite of tools that will enable central banks to explore how a CBDC could freely interoperate with third-party card and real-time payment networks – supporting both seamless consumer experiences and day-1 integration with the security services that exist on those networks.

At Mastercard, we strongly believe that CBDCs will be most successful where central banks leverage the knowledge, experience, and innovations of the private sector. Many central banks have already implicitly recognized this in their focus on two-tier CBDCs, where commercial banks and Fintechs facilitate distribution of the CBDC to end users. If CBDCs leverage existing payment infrastructure, rails, and endpoints, central banks can provide a seamless interface, simplify usage, facilitate mass consumer adoption, and lower their up-front investment. Security will be enhanced even further if central banks take advantage of the decades that private players have dedicated to building the tools needed to secure modern retail payment systems.

Our Cyber & Intelligence leaders are ready to engage in a deeper discussion and explore innovative ways we might help bring your vision to life.

With our more than 50 years of experience, and countless security capabilities beyond those discussed here, Mastercard is eager to partner with central banks to help them achieve their CBDC objectives. We hope this brief overview prompts some fresh ideas on strategies to support the development of secure and trustworthy CBDC systems. Our Cyber & Intelligence leaders are ready to engage in a deeper discussion and explore innovative ways we might help bring your vision to life.

1. Boar, C, H Holden and A Wadsworth (2020): "Impending arrival: a sequel to the survey on central bank digital currency", BIS Papers, no 107, January 2020.
2. https://www.bis.org/speeches/sp190322.pdf
3. https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf
4. Cybersecurity Ventures, 2021 Report: Cyberwarfare In The C-Suite, January 21, 2021.
5. IBM Security, Cost of a Data Breach Report, conducted by Ponemon Institute, 2019.
6. Mastercard's Internal Decision Management Platform, Declined authorization attempt.