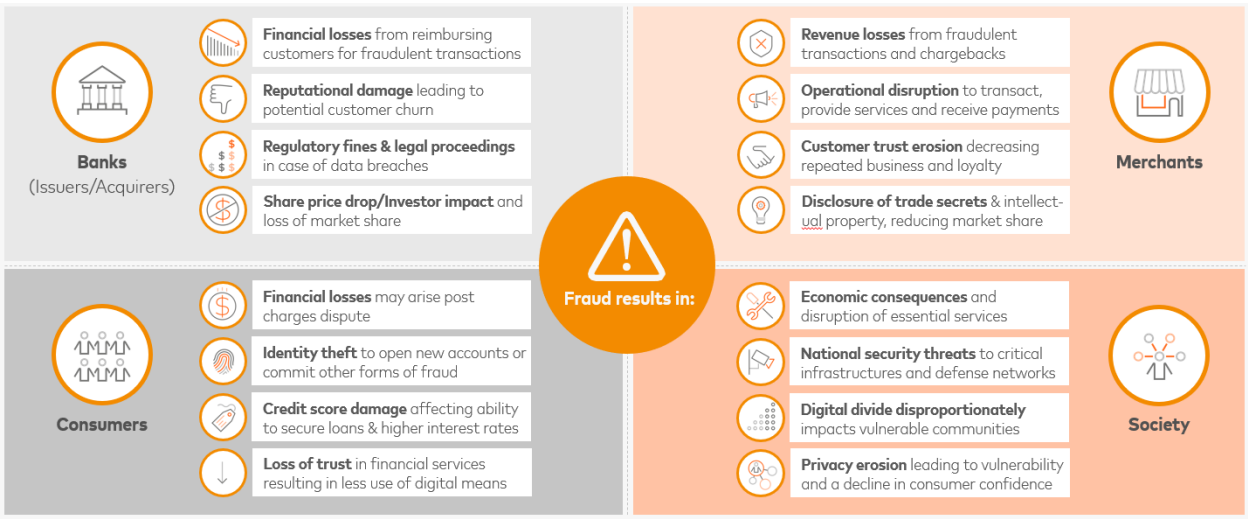
Mastercard response to the Basel Committee on Banking Supervision's Discussion Paper on Digital fraud and banking: supervisory and financial stability implications

February 2024

Mastercard supports and welcomes the Basel Committee's discussion paper on digital fraud and is excited to share its learnings and experiences to inform the discussions on how to address such a relevant topic. Being a global payments technology company processing card transactions in more than 210 countries and territories, we have witnessed firsthand how digital fraud has been proliferating and are active in its prevention.

Fraud often targets the most vulnerable populations, including the elderly and SMEs. It takes many different forms and can occur via many different vectors in a modern payment system. It erodes trust in the financial system and imposes serious costs to individual stakeholders and the society (as highlighted below), demanding policymakers' attention.



Recognizing this problem, Mastercard has been at the forefront of the issue, dedicating significant resources to ensuring the security of our network against an array of threats. In the last five years, Mastercard has invested $7 billion in cybersecurity to combat digital fraud, among other risks.

In line with Mastercard's expertise, below we provide answers to the Committee's questions from a retail payments perspective. While we do not have sufficient visibility to answer questions related to financial stability and/or prudential transmission channels from digital fraud to the banking system we are well

positioned to provide more in-depth insight into fraud vectors and fraud prevention strategies. We are eager to continue the discussion with the Committee beyond the present reply.

Q1. Do you agree with the features and categories of digital fraud? Are there additional financial stability and/or prudential transmission channels from digital fraud to the banking system?

Post-pandemic, the increasing adoption of digital payments has significantly expanded the attack surface for fraudsters, which alongside the advent of new payment systems (some lacking advanced fraud prevention capabilities) contributed to the proliferation of digital fraud and the creation of new risks. For example, some digital wallets add a layer of opacity for merchants, creating new challenges around disputed payments and refund abuse, while the delayed nature of Buy Now Pay Later (BNPL) payments has let fraudsters make several payments using stolen card details before fraud can be identified.

New technologies, like Generative AI, are making these problems even worse by lowering the barrier of entry for less sophisticated fraudsters to do digital harm. New large language models (LLMs) enable social engineering to be faster and more effective at scale. For example, voice deepfakes[1] are being used in vishing campaigns over the phone requesting transfers of funds, while video deepfakes of realistic looking AI-generated videos posing as celebrities[2] endorse investments in nonexistent (illegal) platforms. The lower entry barrier is likely to also contribute to a global rise in ransomware attacks.

Below, we provide key typologies of retail payments fraud that Mastercard observes. These are split in the three stages of a transaction: before (pre), during and after (post). The left-hand side of the infographics presents the steps in each transaction, while the right-hand side provides examples of fraud types (and connected enabling cyber-attacks) that can materialize in each step.

[1] Today, 3 seconds of audio suffice to clone voice using AI (https://techmonitor.ai/technology/ai-and-automation/vall-e-synthetic-voice-ai-microsoft).
[2] The recent example of deepfakes of singer Taylor Swift were followed by calls for legislation.

Pre-Transaction

Network Threats

Onboarding

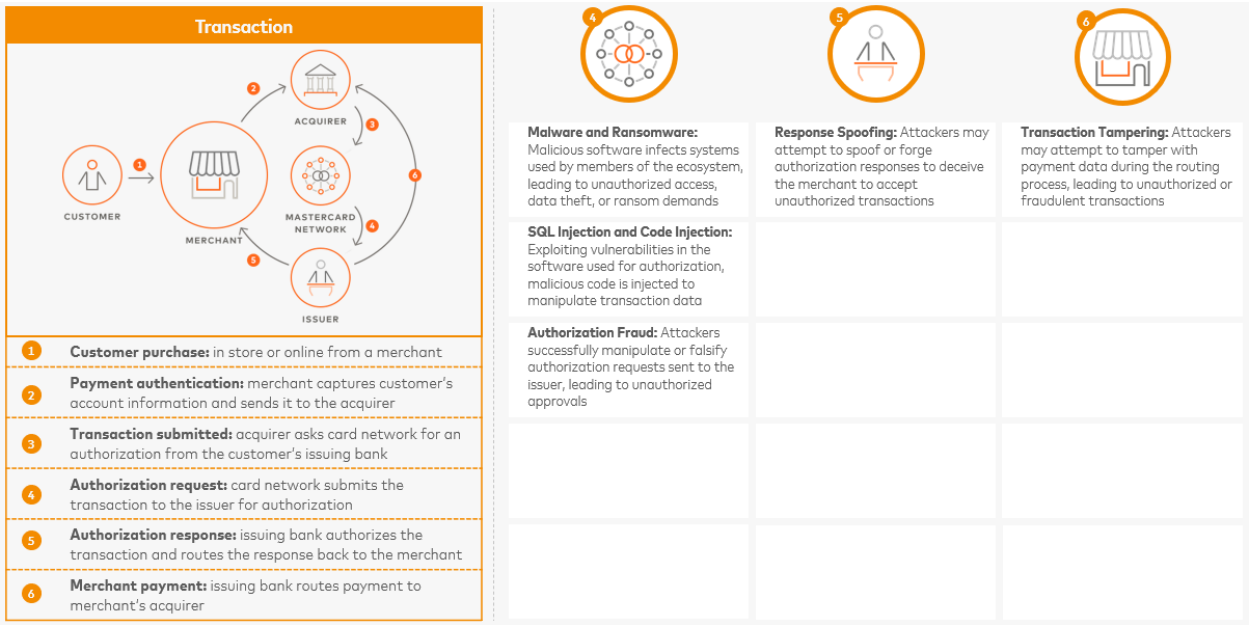
1. **Deterrence of Network Threats:** The network orchestrator must work continuously to ensure the security of the network and of its participants
2. **Customer onboarding:** The consumer applies for a debit, credit, or prepaid card from an issuer, provides personal information and gets approaved
3. **Merchant:** submits business information to acquirer, verifies identity and sets up a merchants account

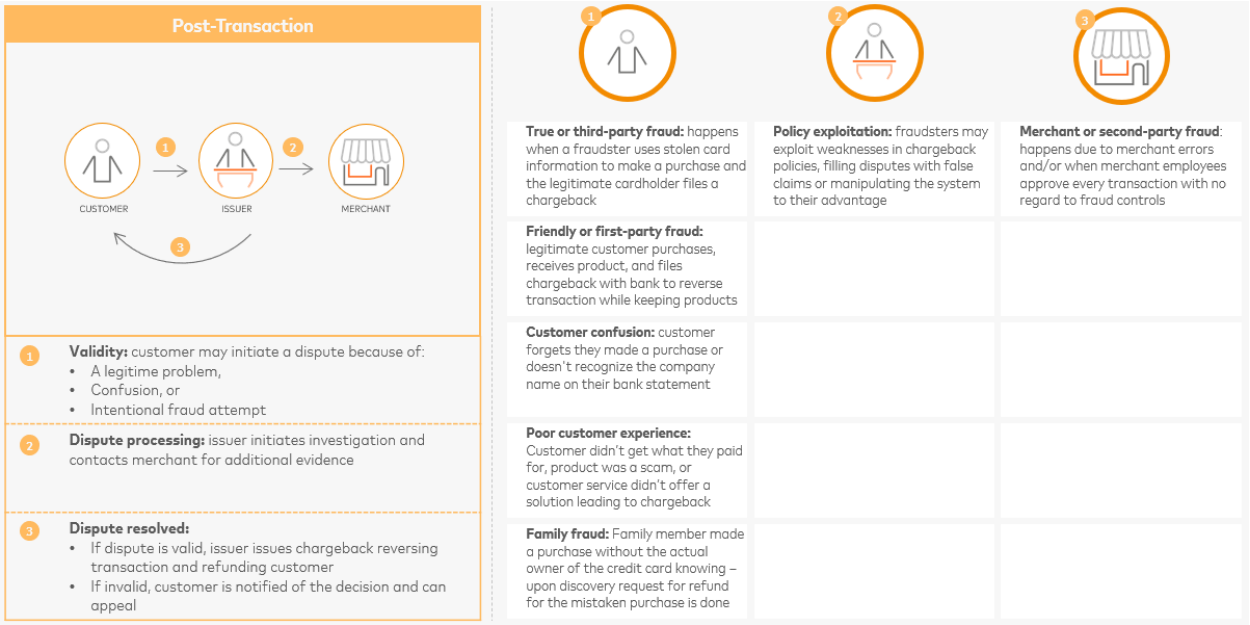
1	2	3
Credential Stuffing: Using automated tools to try large volumes of username-password combinations, taking advantage of individuals who reuse credentials	**Account Takeover (ATO):** Fraudster takes over account through phishing attacks, purchasing stolen personal identity information on the dark web, password cracking, etc.	**Merchant Identity Theft:** Fraudsters may use stolen or fake identities to establish a merchant account with acquirers
Packet Sniffing: Capturing and analyzing data packets passing through the network to extract sensitive information like card numbers	**Synthetic Identity Theft:** Fictional identity created by combining real and fake information from different sources to establish a fraudulent credit profile	**Falsifying Business Information:** Providing inaccurate details about the business, such as financials or transaction volume, to secure approval from the acquirer
Point-of-Sale (PoS) Malware: Targeting the systems where card transactions are processed, aiming to steal card data during the payment process		**Phishing for Account Credentials:** Acquirer login credentials can be targeted through phishing attacks, compromising the security of merchant accounts

Transaction

1. **Customer purchase:** in store or online from a merchant
2. **Payment authentication:** merchant captures customer's account information and sends it to the acquirer
3. **Transaction submitted:** acquirer asks card network for an authorization from the customer's issuing bank
4. **Authorization request:** card network submits the transaction to the issuer for authorization
5. **Authorization response:** issuing bank authorizes the transaction and routes the response back to the merchant
6. **Merchant payment:** issuing bank routes payment to merchant's acquirer

1	2	3
Card Skimming: Illegally obtaining credit card information by placing a device on ATMs, point-of-sale terminals, or other card readers	**Data Interception:** If the transmission is not secure, attackers could intercept the data during transit, leading to unauthorized access and potential misuse	**Identity Spoofing:** Fraudsters impersonate the acquirer when submitting authorization requests, tricking card networks and issuers into approving transactions
Social Engineering: Manipulating individuals into divulging confidential information, often by posing as a trustworthy entity	**Man-in-the-Middle Attacks:** Cybercriminals can intercept communication between merchant and acquirer, gaining unauthorized access to customer information	**Manipulation of Transaction Details:** Fraudsters alter details within the authorization request to make them appear legitimate, leading to unauthorized approvals
Lost or Stolen Cards: Physical theft of a credit card can lead to unauthorized transactions	**Phishing:** Fraudsters might use deceptive emails or communication to trick merchants into disclosing customer account information, posing as the acquirer	
Shimming: Interception and/or a manipulation of information flowing between a card and the chip interface of a card reader that is relayed to another device		





In addition to the typologies above, it is also worthwhile mentioning logical attacks on Automated Teller Machines (ATMs). These comprise coordinated action aimed at gaining access to the ATM computer system, manipulating, or extracting data, and controlling the dispensing function. The most common attack is the Black Box (or jackpotting): this is carried out either by connecting an unauthorized external device to the ATM or by injecting malware into it, with the aim of sending commands directly to the ATM cash dispenser so that it ejects cash.

Mastercard publishes regularly additional information on the types of fraud we observe. Our latest edition of the "The Update" provides additional relevant insights.[3]

[3] https://b2b.mastercard.com/news-and-insights/the-update/issues/the-update-edition-2/

Q2. What other data sources could the Committee consider when assessing the risks of digital fraud?

In addition to those highlighted in the report, we suggest the Committee also review the regular reports published by international law enforcement agencies such as the FBI[4] and Europol,[5] as well as fraud statistics compiled by institutions such as the Federal Trade Commission,[6] and market participants including Juniper Research,[7] Regula,[8] ACI Worldwide,[9] and Paypers[10].

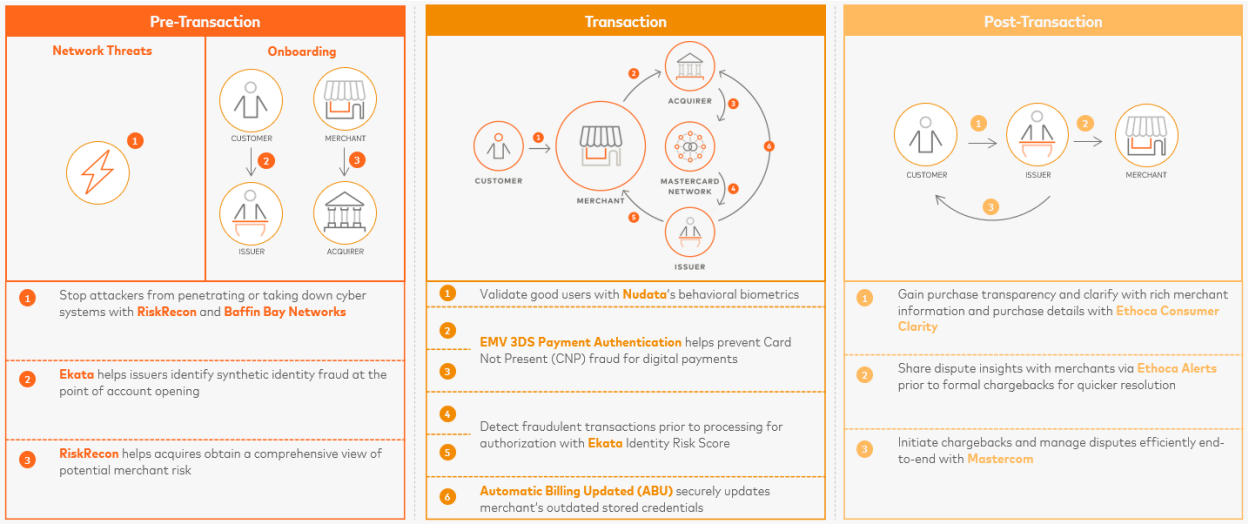
Q3 Are there any additional, banking-specific, initiatives on digital fraud that could be pursued by the Committee?

The growing speed and sophistication of these threats demand a coordinated and collaborative response from the public and private sectors.

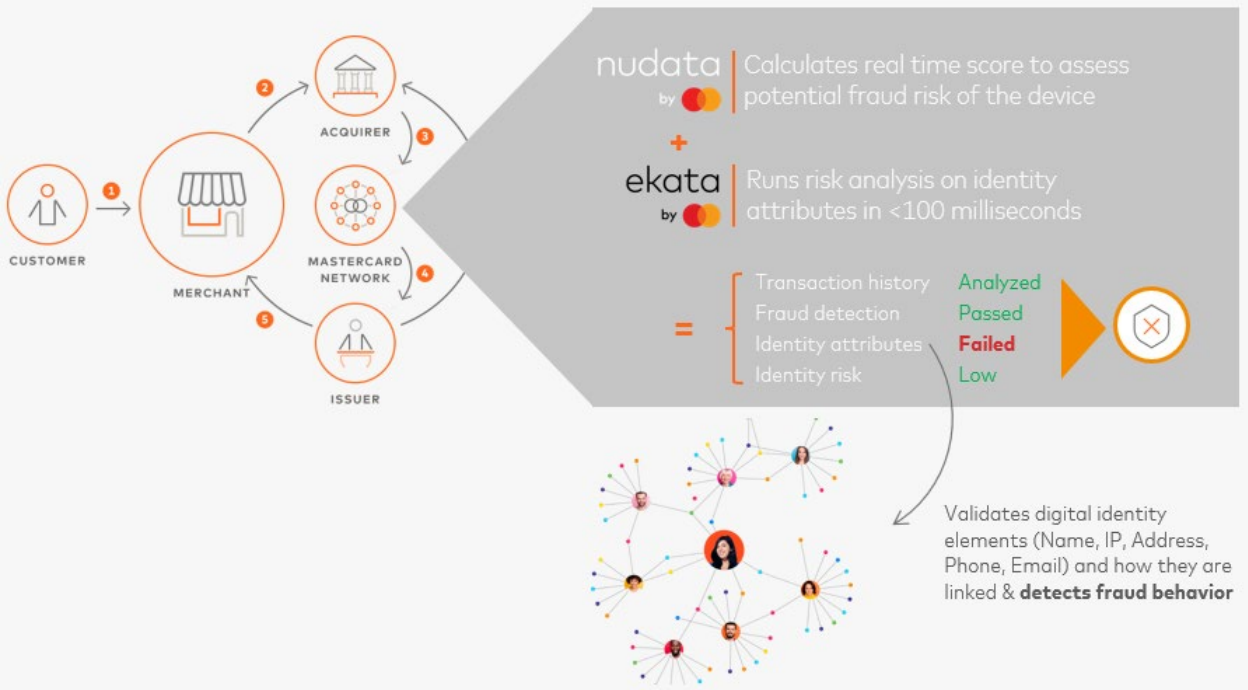
Mastercard has been committed to do its part, leveraging the latest developments and technological breakthroughs to mitigate fraud risks. Selected acquisitions and investments have enabled Mastercard to have access to innovative technologies to address new risks posed by new payment methods and AI, while partnerships with Universities and Law Enforcement allow access to cutting edge investigation and insights into fraud detection and consumer protection. Mastercard has also retained skilled staff through internal talent development and acquisitions of vendors focused on specific areas of the (cyber)security value chain.

These investments and partnerships have been crucial to the reduction of fraud rates that the Committee has highlighted in its report. This reduction is the result of our multi-layered end-to-end approach to network security which provides support to the ecosystem at every step of a card payment transaction (before, during and after) with dedicated tools (shown below).

[4] FBI's Internet Crime Complaint Center (IC3): https://www.ic3.gov/
[5] https://www.europol.europa.eu/cms/sites/default/files/documents/Spotlight-Report_Online-fraud-schemes.pdf
[6] https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports
[7] https://www.juniperresearch.com/press/ecommerce-losses-online-payment-fraud-48bn
[8] https://www.businesswire.com/news/home/20230427005427/en/One-Third-of-Global-Businesses-Already-Hit-by-Voice-and-Video-Deepfake-Fraud
[9] https://investor.aciworldwide.com/news-releases/news-release-details/app-scams-emerge-top-payments-fraud-threat-fraudsters-changing
[10] https://thepaypers.com/reports/fraud-prevention-in-ecommerce-report-2023-2024/r1265410



To illustrate the value added of these tools, we provide the following example. If a fraudster is using credit card details from Jane (a primary school teacher in London) bought on the dark web to acquire hardware appliances in Sydney using a different IP than Jane's, our tools nudata and ekata support the detection of fraudulent behavior as per below.[11]



Mastercard continues to dedicate significant resources to ensuring the security of our network by also developing proprietary tools. We recently announced a new advanced AI model – Decision Intelligence Pro –, which will allow banks to better assess suspicious transactions in real-time and determine whether they are legitimate or not. This proprietary algorithm is trained on our own 125 billion yearly transactions data. The data helps AI understand relationships between merchants

[11] For additional use cases and examples of tools on fraud prevention, please refer to https://nudatasecurity.com/resources/papers-and-reports/paladin-vendor-report-2023-fraud-prevention/.

and predict where fraudulent transactions are taking place. Our algorithm uses the history of a cardholder's merchant visit as the prompt to determine whether the business involved in a transaction is a place the customer would likely go. This process happens in just 50 milliseconds. This new transaction decisioning technology can help financial institutions improve their fraud detection rates by 20%, on average. The algorithm will enable banks to eliminate much of the costs devoted to assessing illegitimate transactions. The true potential of this technology is in its ability to identify fraudulent patterns and trends to predict future types of fraud that are not currently known within the payments' ecosystem.

In addition, Mastercard also has tools that act as a second layer of defense. Many issuers may not even realize their systems have been compromised until the damage is done. Mastercard Safety Net is a solution to combat this threat. It helps protect issuers from large scale fraud events where hackers may have disabled their internal fraud protections. As an additional line of defense, Safety Net monitors transactions at the network level independent from issuers systems. It scans the globe for unusual or abnormal activity and behaviors in real time, across all markets, card products, and payment channels. Safety Net systematically layers advanced intelligence to assess the risk of large-scale attacks in over 200 million transactions a day. It continuously monitors transaction data using AI to identify and surgically isolate threats, all within about 25 milliseconds. Since 2018, Safety Net has saved issuers over 13 billion dollars of potential fraud losses.

We look forward to engaging with the Committee to detail how our tools can further support the banking system in fraud prevention.

As shown by the examples above, fraud prevention entails continuous investment. This requires that not only participants have an interest and incentive to invest in protecting the payments' ecosystem but also the existence of an orchestrating body to ensure that underlying issues in the defensive armor are addressed. In Mastercard's experience this means that a sustainable commercial model is integral to the long-term security of a payments network. A myopic focus on cost reduction of payments, whether by private actors in the case of some P2P or digital wallet offerings, or the public sector through mandated participation in well intentioned Digital Public Infrastructure (DPI) projects, may have the unintended consequence of increasing fraud risks. Moreover, data localization requirements while intended to support law enforcement and ensure data protection/privacy, restrict the ability to create global models to detect/respond to fraud treats.