February 16, 2024

Pablo Hernández de Cos, Chairman
Basel Committee on Banking Supervision
Centralbahnplatz 2
4051 Basel, Switzerland

RE: Basel Committee on Banking Supervision Discussion Paper "Digital fraud and banking: supervisory and financial stability implications"

Dear Mr. Hernández de Cos:

The Bank Policy Institute,[1] through its technology policy division BITS,[2] appreciates the opportunity to respond to the discussion paper, **"Digital Fraud and Banking: Supervisory and Financial Stability Implications**," issued by the Basel Committee on Banking Supervision.[3] We encourage the Committee to consider the recommendations in this response as it continues to update its discussion paper and assess the implications of fraud to the banking ecosystem.

Fraud management is an important priority for all participants in the global financial system, as well as a concern for the customers the financial system serves. The Bank Policy Institute has been working with banks for nearly three decades to address critical fraud challenges and facilitate efforts by industry and government stakeholders to combat fraud. Examples of BPI-led initiatives include developing customer education programs on fraud, identifying effective practices for detecting fraud, partnering to implement fraud intelligence sharing services and implementing strategies to mitigate check fraud, among many other actions.

In recent years, the financial system has experienced a rise in fraud attacks due to the increased availability of stolen access credentials, the proliferation of synthetic identities, a substantial increase in the sophistication of scams and social engineering and a surge in check fraud. At the same time, banks

[1] The Bank Policy Institute is a nonpartisan public policy, research, and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost 2 million Americans, make nearly half of the nation's small business loans and are an engine for financial innovation and economic growth.

[2] BITS – Business, Innovation, Technology, and Security – is BPI's technology policy division that provides an executive-level forum to discuss and promote current and emerging technology, foster innovation, reduce fraud, and improve cybersecurity and risk management practices for the nation's financial sector.

[3] Digital fraud and banking: supervisory and financial stability implications (bis.org)

have expanded their digital banking services as customer preferences have evolved. Along with this growth, banks have invested significant resources in enhancing fraud controls and will continue to invest in protecting their customers as a key focus area.

I. Growth of Digital Banking

Digital banking services in the United States have significantly grown in the last few. A recent report by Cornerstone Advisors suggests that, as of 2022, 78% of adults in the U.S. prefer to bank via a mobile app or website.[4] The number of digital banking users in the United States is expected to grow year-on-year through 2025 with the number of digital banking users in the country forecasted to reach almost 217 million by 2025.[5]

Banks offer digital banking for several reasons, including:

- **Convenience for Customers:** Online banking allows customers to access their accounts and perform various transactions from the comfort of their homes or on the go. This convenience is a significant draw for customers who prefer the flexibility of managing their finances without the need to visit a physical branch or who cannot visit a branch during normal business hours.
- **24/7 Access**: Online banking provides continuous access to account information and services, 24 hours a day, seven days a week. This ensures that customers can check their balances, transfer funds, and conduct other transactions at any time, even outside regular banking hours.
- **Efficiency and Automation:** Online banking streamlines many banking processes, reducing the need for manual intervention. Automated systems can handle routine transactions, making operations more efficient, reducing the likelihood of human errors, and improving customer satisfaction.
- **Expanded Customer Reach:** Online banking enables banks to reach a broader customer base, including those who may not have easy access to physical branches. This is particularly important for attracting younger customers who are more accustomed to digital transactions.
- **Competitive Advantage:** In the modern banking landscape, offering online services is a competitive necessity. Banks that provide robust and user-friendly online banking platforms are more likely to attract and retain customers in a market where digital services are increasingly expected.
- **Enhanced Security Features:** Online banking platforms often incorporate advanced security measures to protect customer information and transactions. While security is a concern for customers, the implementation of features like encryption, multi-factor authentication, and fraud detection helps build trust in online banking systems.
- **Innovative Features and Services:** Online banking allows banks to introduce new and innovative features to meet evolving customer needs. This may include mobile banking apps, budgeting tools, investment platforms and other value-added services.
- **Expedited and Cost-Effective Communication:** Banks can use online channels for expedited and cost-effective marketing and communication. They can provide customer education, transaction, account activity and fraud alerts and notifications as well as promote new products, services and

[4] Mobile Banking Adoption In The United States Has Skyrocketed (But So Have Fraud Concerns) (forbes.com)

[5] The Current State of Online Banking - Insider Intelligence (businessinsider.com)

special offers through digital channels, reaching a wider audience at a lower cost and greater speed compared to traditional methods.

In summary, online banking offers a range of benefits, including improved customer convenience, enhanced protection and security, cost savings opportunities, expanded market reach and the ability to stay competitive in a rapidly evolving financial landscape.

II. Enhanced Digital Fraud Controls for Digital Banking

With the growth in digital payment and banking services, a need for increased fraud controls has arisen. Banks have made significant investments in fraud controls for the digital channel over the past several years.[6] Digital banking services provide an opportunity for stronger security controls that enable advanced fraud detection capabilities. Many of these controls are more advanced and offer greater security than non-digital channels due to their device-based controls and enhanced authentication that often cannot be leveraged on other channels.

Banks implement a range of controls for online fraud prevention and detection to safeguard their customers' sensitive information and the integrity of online transactions. These controls involve a combination of technology, security protocols and monitoring systems. Banks also deploy in-depth defense strategies for digital channels, which includes multiple layers of security to protect their customers. Common controls used by banks include:

(1) Digital Fraud Risk Monitoring Systems

- **Fraud Detection and Prevention Models:** Sophisticated algorithms and systems are employed to monitor account activity in real time. Unusual patterns, large transactions or suspicious behavior trigger alerts for further investigation. These systems help to detect and prevent fraudulent transactions by identifying abnormal behavior.
- **Geolocation and Device Recognition:** Banks may use geolocation data and device recognition technology to identify the location and characteristics of the device used for online banking. Deviations from typical usage patterns may trigger alerts. This is a key control that is unique to digital users and enhances security by identifying potential unauthorized access or fraudulent transactions.
- **Behavioral Biometrics Analysis:** Behavioral biometrics for fraud detection involves analyzing and identifying unique patterns of behavior or activities associated with individuals to verify their identities or detect fraudulent activities. Unlike physical biometrics (such as fingerprints or iris scans), which rely on physical traits, behavioral biometrics focuses on behavioral characteristics. These patterns can include keystroke dynamics, mouse movements, voice patterns and even the way individuals interact with devices and systems.
- **Transaction Risk Analysis:** Banks analyze transaction characteristics, including amount, frequency and recipient, to assess the risk associated with each transaction. This control identifies and blocks potentially fraudulent transactions based on predefined risk parameters.
- **Fraud Alerts:** The systems above are used to trigger alerts, and customers are promptly notified of potentially fraudulent activities. This rapid response can help prevent further unauthorized access.

[6] PwC's Global Economic Crime and Fraud Survey 2022

- **Customer Account Activity Monitoring:** Online banking allows users to monitor their account activity regularly. This real-time access to transaction history enables users to quickly identify and report any unauthorized or suspicious transactions.

(2) Security and Enhanced Customer Authentication

- **Encryption:** Encryption is used to secure the transmission of sensitive data between the user's device and the bank's servers. This ensures that information such as login credentials, account numbers and transaction details is protected from unauthorized access. This control prevents interception and eavesdropping on communication channels.
- **Secure Socket Layer (SSL) Certificates:** SSL certificates ensure secure communication between the user's browser and the bank's website. This encryption protects sensitive information during transmission. This control safeguards against man-in-the-middle attacks and unauthorized access.
- **Multi-Factor Authentication (MFA):** MFA requires users to provide multiple forms of identification before accessing their accounts or higher risk functions such as an international payment beneficiary. This often includes a combination of passwords, one-time codes sent to registered devices or physical authentication devices. This adds an extra layer of security by ensuring that even if one form of authentication is compromised, the account remains protected.
- **Biometric Authentication:** Some online banking systems incorporate biometric authentication methods such as fingerprint or facial recognition. Biometrics provide a high level of security by uniquely identifying individuals based on physical or behavioral characteristics.
- **Automatic Logout and Session Management:** Online banking sessions often have timeout features that automatically log out users after a period of inactivity. Session management controls prevent unauthorized access to an active session. This helps to mitigate the risk of unauthorized access when a user's device is left unattended.
- **Account Lockout Policies:** Implementing policies that lock out user accounts after a certain number of failed login attempts helps protect against brute force attacks. These policies also help manage automated bot attacks and automated agent access, which can affect customer accounts. This prevents attackers from systematically attempting to guess passwords and accessing accounts.

(3) Governance and Oversight

- **Regular Security Audits and Assessments:** Banks conduct regular security audits and assessments to identify vulnerabilities and ensure that their systems are up-to-date and compliant with industry standards. This is a proactive way to identify opportunities to enhance controls and ensure ongoing resilience against evolving threats.
- **Measurement and Monitoring:** Banks have a suite of metrics that measure and monitor the digital fraud experience. Typically, risk tolerance thresholds will be applied to ensure root causes are identified and risk mitigation strategies are deployed to address risk tolerance breaches.
- **Control Testing:** Banks conduct regular control testing to assess the design and operating effectiveness of digital fraud controls. This is a proactive activity to continuously improve digital banking fraud control environments.
- **User Education and Awareness:** Banks provide education and awareness campaigns to inform users about common fraud risks and best practices for securing their online accounts. This activity empowers users to recognize and avoid phishing scams and other fraudulent activities.
- **Enterprise Fraud Policy:** A fraud policy at a bank is a set of guidelines and procedures designed to prevent, detect, and respond to fraudulent activities within the financial institution. The primary

goal of a fraud policy is to establish a framework that helps protect the bank, its customers, and stakeholders from financial losses, reputational damage, and other adverse effects associated with fraudulent behavior.

These controls work together to create a multi-layered defense against digital fraud, enabling banks to manage digital fraud effectively. Digital transaction fraud rates are often managed more effectively than paper transactions (i.e., checks), making digitization of legacy payment methods an ongoing priority for banks. Due to the enhanced controls that the digital channel provides many banks encourage customers to interact in digital banking channels. In some cases, banks encourage customers to use digital channels over other channels and will even guide customers through the digital experience, if a specific transaction can be done online.

III. Banks Continued Investment in Controls to Protect Customers

Protecting customers and their accounts from fraudulent activity is of critical importance to banks. Costs to consumers have been increasing. Consumers reported losing almost $8.8 billion to scams and fraud in 2022, up 30 percent over 2021's losses, according to newly released numbers from the Federal Trade Commission. This means extensive investment in people and technology to protect customer accounts. Juniper Research predicted that in 2022, banks spent $9.3 billion annually on fraud detection and prevention tools.[7] According to the 2022 6th Annual True Cost of Fraud Study, U.S financial services firms' fraud costs continue to rise, up to 22.4% higher since early 2020. The cost of fraud is highest among U.S. banks, where every $1 of fraud loss costs $4.36 mainly due to investments in technology, people and processes to better prevent fraud and assist victims once fraud has occurred.

Fraud risk management will continue to be a focus area for banks, especially with the continued expansion of digital banking.

IV. Responses and Recommendations to the Questions raised in the Discussion Paper

Regarding the specific questions raised by the Committee in the paper, we have the following recommendations and comments.

(1) Q1 Part 1: Do you agree with the features and categories of digital fraud?

After reviewing the definition of digital fraud in the discussion paper, we put forth four recommendations we would make to the Committee.

A. Recommendation: Leverage existing frameworks for defining fraud risk, which are irrespective of the channel by which it occurs.

It is strongly recommended the Committee leverage existing frameworks for defining fraud risk as an operational risk. In the paper, the Committee specifically states that, "Digital fraud is related to, but different from, operational risk/resilience, cyber risk and/or social engineering." However, there is industry-wide acceptance of fraud risk as an operational risk. Irrespective of the channel through which

[7] The banking industry's multi-billion dollar fraud problem—and how to solve it (bai.org)

it occurs, fraud is managed as an operational risk for most banks today. Additionally, existing governance models and frameworks already exist for managing banks' operational risk.

One example of this is supported by the approach to annual CCAR stress testing and the Office of the Comptroller of the Currency (OCC) in the United States, which states in Bulletin 2019-37:

> Fraud risk is a form of operational risk, which is the risk to current or projected financial condition and resilience arising from inadequate or failed internal processes or systems, human errors or misconduct or adverse external events. Operational risk management weaknesses can result in heightened exposure to fraudulent activities, which can increase a bank's exposure to reputation and strategic risks. Failure to maintain an appropriate risk management system could expose the bank to the risk of significant fraud, defalcation (e.g., misappropriation of funds by an employee) and other operational losses[8].

Another example is the Office of the Comptroller of the Currency in the United States has a set of fraud risk-management principles that apply to the banks it supervises. This guides the expectations of banks' fraud risk management frameworks.

Highlights of the principles published in OCC Bulletin 2019-37 are: [9]

- A bank should have sound corporate governance practices that instill a corporate culture of ethical standards and promote employee accountability.
- A bank's risk management system should include policies, processes, personnel and control systems to effectively identify, measure, monitor and control fraud risk consistent with the bank's size, complexity and risk profile.
- A bank's risk management system and system of internal controls should be designed to
  - prevent and detect fraud; and
  - appropriately respond to fraud, suspected fraud, or allegations of fraud.
- Bank management should assess the likelihood and effect of potential fraud schemes and use the results of this assessment to inform the design of the bank's risk management system.
- Senior management and the board of directors should measure, monitor and understand fraud losses across the enterprise and employ tools that appropriately quantify and assess loss experience and exposure.
- Control reviews and audits should include fraud risk as part of their assessments.

Other U.S. agencies have similar guidance that they use in supervisory efforts, that can be used for all categories of fraud, not just digital.

Furthermore, bank capital requirements already reflect operational risk losses as part of the stress capital buffer (SCB) requirement, which is determined by the Federal Reserve Board as part of the annual supervisory stress test. The FRB has stated in its supervisory stress testing methodology that operational risk losses capture events including internal fraud, external fraud, employment practices and workplace safety, clients, products and business practices, damage to physical assets, business disruption and

[8] https://www.occ.treas.gov/news-issuances/bulletins/2019/bulletin-2019-37.html#ft2

[9] Operational Risk: Fraud Risk Management Principles | OCC (treas.gov)

systems failures, and execution, delivery, and process management and is based both on industry-wide and individual bank historical losses. The FRB's most recent supervisory stress test results reflected approximately $185 billion of operational risk losses, in the aggregate for large banks which are a direct input into SCB requirements. In addition, the FRB stated in its most recent Supervision and Regulation Report that the banking sector remains sound overall and that banks continue to report capital above regulatory minimums. We observe that banks are sufficiently capitalized, as evidenced by the recent FRB stress test results, statements from the FRB and the banking systems' collective ability to withstand real-world events, including the COVID-19 pandemic as well as the more recent string of bank failures.

Establishing new rules or frameworks when existing ones are in place in many jurisdictions is not recommended.

B. Recommendation: Acknowledge how digital fraud is inherently captured in existing fraud classification models and taxonomies, negating the need for a separate, new definition or classification model.

Although fraud risk is accepted as a form of operational risk, the lack of consistently adopted classification models or systems across fraud *types* has been a persistent challenge.

The benefit of a common lexicon and categorization model can't be underestimated for tracking fraud. Over the past few years, there have been several efforts and progress made to establish categorization and classification models. An example would be the Federal Reserve Fraud Classifier model, which could be drawn from or built upon for the purposes of this discussion.

This model incorporates multiple categories of fraud and was developed with input from agencies and banks. It addresses or expands upon some of the proposed categories the Committee is requesting input on. The model asks three questions and each question provides additional context to the fraud event. The three questions are:

1. Who initiated the payment? The initiator is either classified as an authorized party or an unauthorized party.
2. How was the fraud executed? For example, the initiator could have been manipulated if they are the victim – or may have hacked an account if they're the fraudster.
3. What tactics were used? This is the most detailed classification level, identifying exactly how the fraudster succeeded in committing the fraud (for example, through a relationship scam).

Another example is the EBA Fraud Taxonomy.[10] This is a classification system or framework developed by the European Banking Association to categorize and describe different types of fraud in the banking and financial sector. This taxonomy helps standardize the identification and reporting of fraud incidents, providing a common language and set of definitions for financial institutions, regulatory authorities and other stakeholders. This model encompasses fraud across multiple bank channels. There could be an opportunity for the Committee to harmonize these models in future work.

[10] Expert Group on Payment Fraud-related Topics (abe-eba.eu)

As far as classification models are considered, one category that could use additional input is related to fraudulent application classification. The two areas of fraudulent application that should be addressed are:

1. Third-Party Fraud Application: Using stolen personal information to submit credit card applications, open bank accounts, or apply for loans without the victim's knowledge or consent.
2. Synthetic Identity: Creating fictitious identities by combining real and fake information. Unlike traditional identity theft, where a criminal steals the personal information of a specific individual, synthetic identity fraud involves the fabrication of entirely new identities. This makes it a challenging form of fraud to detect and prevent.

C. Recommendation: Draw a clear distinction between "fraud" and "scams," and the defining features of each.

As the discussion paper acknowledges, fraud can take the form of many different attack vectors. As it relates to banking, digital is a channel where fraudulent monetization occurs, not a fraud type in and of itself. However, whether that monetization is a result of an *authorized* or an *unauthorized* transaction is a key distinction and has implications for how the event is detected, how the risk is mitigated and subsequent liability structure(s) that may be considered by standard setters.

To illustrate this point, consider the following:

- A payment transaction made as a result of an account holder being manipulated to *authorize* a payment to an account the consumer believes belongs to a legitimate payee (e.g., romance scam). This is referred to as a scam, and greater authentication and anti-fraud mechanisms employed by the customers' bank have little effect when the customer has been convinced to hand over their money and/or credentials. Scam detection and risk mitigation require a different approach in this scenario than in an *unauthorized* payment transaction scenario, where authentication controls can detect that the account has been taken over and can prevent money movement.
- In the United States, consumer protections are defined by Regulation E for electronic payments. Reg E states that when a transaction is *unauthorized*, it is considered fraud and the customer is not liable. Scams where a customer is tricked into authorizing the transaction are not covered by Reg E.

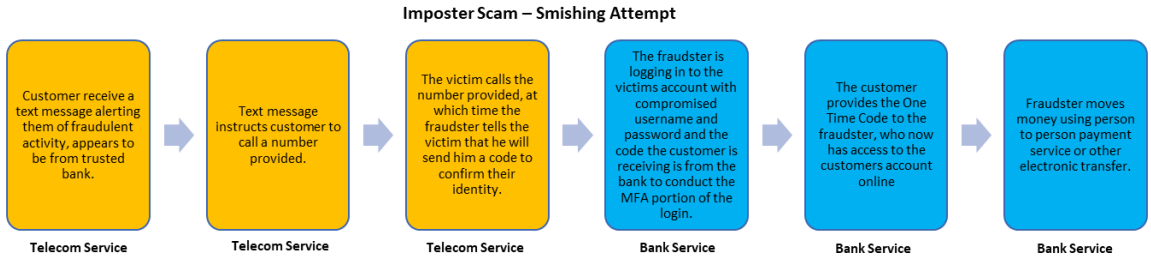
The examples above illustrate why any proposed definition or classification of fraud should have a holistic review in the context of what effect it might have on the current practices for each of the various payment types governed under different laws and regulations. Moreover, a universal definition for scams that is separate and distinct from fraud would serve to enable banks to begin tracking and reporting on the volumes and losses associated with each in a consistent manner and would enable the industry to better position itself for mitigating both.

D. Recommendation: Specifically acknowledge the role of fraud enablers and the cross-industry aspect of digital fraud risk management.

Monetization is often the final step in a larger overall scheme, where the malicious actor has done work ahead of time to gather information as well as user credentials or has social-engineered a victim to get what they need to take money from their account. The Committee should draw a distinction between the digital activities used to gather or steal credentials (access or payment), where the bank is oftentimes not directly involved and the use of the stolen credentials. Two attack examples are defined in Figures 1 and 2:

Figure 1: Imposter Attack Initiated on a Social Network

Figure 2: Smishing



There are layers of activity between the customer and the bank, and there are enablers that play a material role in the steps that occur leading up to the movement of money. The Committee states in the discussion paper that "Digital fraud shall therefore be defined as all fraudulent activities perpetrated by external parties through digital means (e.g., emails, websites, malicious software, etc.) with the aim of stealing banking assets or credentials of bank customers." The Committee should more clearly articulate and differentiate the activities that are enablers of an attack vs the actual event. The examples provided, such as emails, websites, malicious software, etc. are enablers of a fraud or scam attack. It is recommended to define and acknowledge the enablers to articulate their effect more clearly. A list of enablers, although not exhaustive, that should be discussed and included are:

- **Email Phishing:** Fraudsters send emails posing as legitimate entities, such as banks or government agencies, to trick individuals into revealing sensitive information like passwords or credit card details.
- **Spear Phishing**: Targeted phishing attacks where fraudsters customize their approach for a specific individual or organization, often using information gathered from social media or other sources.

- **Vishing (Voice Phishing)**: Fraudsters use phone calls to impersonate legitimate organizations or individuals, attempting to extract sensitive information from the victim.
- **Smishing (SMS Phishing):** Like email phishing but conducted through text messages. Victims may receive fraudulent messages with links or requests for personal information.
- **Malware and Ransomware:** Fraudsters use malicious software to gain unauthorized access to a computer or network. Ransomware encrypts a user's files and demands payment for their release.
- **Man-in-the-Middle Attacks:** Hackers intercept and potentially alter communication between two parties, often without their knowledge, to gain access to sensitive information.
- **Fake Websites and Spoofing:** Criminals create fake websites that mimic legitimate ones to trick users into entering sensitive information. This is often done through deceptive URLs or website designs.
- **Social Engineering:** Malicious actors manipulate individuals into divulging confidential information through psychological manipulation, exploiting human trust and tendencies. Social engineering has become a large driver of scams today, as illustrated in Figure 1 and Figure 2, and is the precursor to money being moved at a bank.
- **Data Compromise:** Occurs when unauthorized individuals gain access to sensitive or confidential information, potentially leading to the exposure, theft, or misuse of that data. This unauthorized access can happen through various means, including cyberattacks, hacking, physical theft, or accidental exposure. Once a data compromise occurs, the compromised information may be used for fraudulent activities, identity theft, or other malicious purposes.
- **Gen AI:** With the ability to autonomously create new, original content, generative AI can be particularly valuable to malicious actors by producing chat responses, synthetic data and even deepfakes at a scale not previously seen. It is also a key threat for its ability 'to perfect' impersonation efforts by malicious actors.

E. Additional Commentary on Proposed Definition of Digital Fraud

a) Separation of Cyber and Fraud Classification

In relation to the categories of fraud as well as features, the Committee should ensure that the definition and categories have a clear differentiation between cyber-attacks and fraud.

As proposed in the discussion paper, category four specifically states:

> *"It can also consist of compromising the bank's information system, obtaining the credentials of an administrative user of the mobile banking application portal and using this access to edit the mobile device number of some customers in order to bypass one-time-password authentication, increase the limits of the customer accounts and access them to conduct fraudulent funds transfers."*

An attack on a specific bank system in which access is restricted to employees of the bank should be considered internal fraud or a cyber-attack (cyber event) based on the attack type. The example given here may enable larger losses for the bank or an ability for the attackers to have higher cash limits, but the root cause is still unauthorized access to the banks' system. For these reasons, it is recommended to keep the Keeping classification of cyber events and fraud events separate.

b) Features Relevant to Digital Fraud

The section of the discussion paper that focuses on the four features of digital fraud and could largely be applied to fraud committed through any channel.

Moreover, although we are in agreement that appropriate authentication technologies do mitigate certain fraud types, and are an important control as stated above in the Security and Enhanced Customer Authentication section of our introduction, it is not accurate to assume, as stated in this section, that digital fraud relies on the inability to authenticate who is at the origin of a transaction, as certain events are at the instruction of the actual consumer who has become a victim of a scam.

(2) Q1 Part 2: Are there additional financial stability and/or prudential transmission channels from digital fraud to the banking system?

An additional area that should be considered when discussing digital fraud is the growth of open banking and the additional risks it brings to the ecosystem, particularly when credential-based access and screen scraping continue to be used by third parties to access consumer financial data.

In the United States, as consumer demand for digital and interactive financial products and services has increased, an increasing number of financial technology firms and other companies have entered the market for consumer financial products and services. Increasingly, however, these entities rely on access to sensitive consumer data held at a financial institution to provide their products and services.[11] Our members welcome the competition brought about by innovative financial technology firms and are prepared to support the ability of bank customers to connect their bank accounts to the third-party apps of their choice including where a data aggregator is used to retrieve the customer's information from the customer's financial institution and share it with the app. But such competition cannot come at the expense of exposing personally identifiable information to the wrong party. It is critical that consumers' personal and financial information remains secure when it is shared between financial institutions and third parties and when it is stored outside of the financial institution. In addition, regulation of the data economy must not create unfair competition by, for example, limiting the imposition of fees by some but not all in the ecosystem.

The banking industry has been working for years to develop technical solutions that enable consumer access to financial data while providing adequate data protection. The financial services industry has collectively advanced the marketplace towards common technical standards for the secure access of consumer-permissioned data. For example, through FDX, a cross-section of banks, third-party fintechs,

[11] *See* U.S. Department of the Treasury Report to the White House Competition Council "Assessing the Impact of New Entrant Non-bank Firms on Competition in Consumer Finance Markets" (Nov. 2022), *available at* Assessing the Impact of New Entrant Non-bank Firms on Competition in Consumer Finance Markets (treasury.gov).

data aggregators, consumer groups and other financial industry groups have aligned around a common API to standardize the security and authentication for data transfer.[12] Through the development, adoption and constant improvement of the FDX API, FDX and its members have made significant progress transitioning from credential-based screen scraping to the FDX API, with over 65 million consumer accounts using the FDX API as of Fall 2023.[13]

Despite the industry's progress, screen scraping remains a widely used method for accessing not only payments account data, but also other types of data that are less accessible through a bank account (such as payroll data), thus enabling data harvesting of credentials to continue. The technology exists today to migrate to APIs, but market participants may never have the incentive to transition to APIs if screen scraping is allowed to continue, including if it is retained in some form as a fallback mechanism.

BPI has long argued that screen scraping and credential-based access should be prohibited at a certain future date for the following reasons.[14]

First, screen scraping, whether using account credentials or a token, does not allow consumers or data providers to control the amount of data they share with third parties and there is no way to ensure that the information "scraped" and maintained by the aggregator does not go beyond what is necessary for the third-party financial app to deliver the services sought by the consumer or what was specifically authorized by the consumer. Additionally, there is the risk that the aggregator or third-party app may continue to collect and store the consumer's data and credentials even after the consumer ceases using the financial app or revokes account access authorization. Several large data aggregators have engaged in this practice and have been required to delete consumer personal financial data that the consumer did not ask the data aggregator to collect but that they retrieved and stored anyway.[15]

---

[12] *See* Financial Data Exchange website at https://financialdataexchange.org/.

[13] *See* FDX Press Release*:* "Financial Data Exchange (FDX) Reports 65 Million Consumer Accounts Use FDX API" (October, 5, 2023), *available at https://financialdataexchange.org/FDX/News/Press-Releases/Financial%20Data%20Exchange%20(FDX)%20Reports%2065%20Million%20Consumers%20Use%20FDX%20API.aspx (last accessed December 24, 2023)*. Almost all FDX Financial Institution (FI) members are using or plan to use the FDX API.

[14] *See*, *e.g.*, BPI comment in response to the High-Level Summary and Discussion Guide of Outline of Proposals and Alternatives Under Consideration for SBREFA: Required Rulemaking on Personal Financial Data Rights issued by the Consumer Financial Protection Bureau pursuant to Section 1033 of the Dodd-Frank Act (Jan. 25, 2023); *See also* BPI-TCH response to the Proposed Required Rulemaking on Personal Financial Data Rights issued by the Consumer Financial Protection Bureau pursuant to section 1033 of the Dodd-Frank Act (Dec. 29, 2023).

[15] For example, in July 2022, a federal judge approved a $58 million settlement of certain data collection and use claims against Plaid, Inc., which provides login services for banking applications, and linking and verification services for various financial technology applications. Plaid also agreed to certain changes to its data collection practices, including deleting data from its systems that was retrieved as part of Plaid's "Transactions" product for users that Plaid can reasonably determine did not connect an account to an application that requested Transactions data; deleting data from its systems for users for whom Plaid is aware that it no longer has valid means that can be used to authenticate with the financial institution; including a prominent reference to Plaid Portal on its website homepage along with a link to the Plaid Portal and a plain-language description of the user

Second, credential-based screen scraping creates opportunities for malicious actors to gain access to a consumer's accounts and commit fraud, or even take over the consumer's account. As former FinCEN Director Kenneth A. Blanco has previously warned, "[i]n some cases, cybercriminals appear to be using fintech data aggregators and integrators to facilitate account takeovers and fraudulent wires. By using stolen data to create fraudulent accounts on fintech platforms, cybercriminals are able to exploit the platforms' integration with various financial services to initiate seemingly legitimate financial activity while creating a degree of separation from traditional fraud detection efforts."[16]

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

To combat digital fraud, a global coordinated effort that addresses several risks is necessary. The following recommendations are areas that the Committee should look to focus on:

A. Recommendation: Establish Cross-Sector Solutions and Frameworks in a unified effort to mitigate fraud and protect consumers.

The issue of combating scams and fraud is a global challenge, one in which banks invest substantial resources to protect their customers and their customers' money. Such a far-reaching challenge demands comprehensive, multi-dimensional solutions. Collaboration across the private and public sectors is crucial to help protect American consumers from criminals who seek to defraud them. We recommend focusing on the following three areas related to cross-sector collaboration.

a) Ensure all sectors are properly held accountable to help mitigate fraud and scams.

Cross-sector involvement, including the telecom industry and social media platforms, is necessary to properly fight digital fraud. A digital fraud scheme is usually complex and coordinated, spanning a large ecosystem of cross-sector players who all have an opportunity to detect and prevent attacks from occurring. To effectively address this fraud, multiple sectors must participate in cross-sector initiatives aimed at preventing attacks against consumers. It is critical that all participating sectors feel compelled and accountable to help protect customers. Banks alone cannot address the problem without collaboration from other industries.

---

controls available; ensuring that its standard Plaid Link flow includes certain disclosures; minimizing the data Plaid stores from users' financial accounts; and enhancing its End User Privacy Policy to provide more detailed information about Plaid's data collection, storage, use, sharing, and deletion practices. Plaid denied the allegations of privacy violations and the settlement agreement does not include any admission of wrongdoing by the company. *Cottle v. Plaid Inc.*, 20-cv-03056-DMR (N.D. Cal. Jul. 20, 2022), available at: Cottle v. Plaid Inc., 20-cv-03056-DMR | Casetext Search + Citator.

[16] Prepared Remarks of FinCEN Director Kenneth A. Blanco, delivered at the Federal Identity (FedID) Forum and Exposition, *"Identity Attack Surface and a Key to Countering Illicit Finance"*, (September 24, 2019), *available at* https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-federal-identity-fedid.

The banking sector is most commonly associated with fraud since the desired outcome of a malicious actor is to steal money from their victim. Examples of the complex and diverse ecosystem can be found in Figures 1 and 2 above and additional context is laid out in the bullets below.

- **Telecom SIM Swapping/Strong Authentication**: Scammers social engineer mobile operators or deceive customer service representatives at a mobile operator to swap a victim's SIM card to gain control of their phone number. This can be used to bypass two-factor authentication and gain access to accounts at banks. The Committee should identify areas that it can work cross-sector to recommend changes such as requiring the use of risk-based, multi-factor authentication.
- **Illicit Use of Mobile Networks:** Scammers send phishing messages via SMS, claiming to be from trusted sources such as banks or government agencies. These messages often contain malicious links or prompts to provide personal information and are the initiation of a digital fraud event. To effectively address digital fraud, the Committee should call on these providers to stop the flow of fraudulent messages in their networks.
- **Illicit Use of Social Networks**: Fraudsters often use social networks to engage with victims by creating fake posts, listings and profiles. This activity is often used for gathering information or creating relationships with a victim. To effectively address digital fraud, the Committee should call on these providers to better educate their consumers, implement technology to identify fraudulent activity and stop crime occurring on their platforms.

According to the U.S. Federal Trade Commission, in 2022 there were 2.4 million consumers who reported being a victim of fraud. It was also reported that consumers lost $1.2 billion because of fraudulent scam activity involving social media. When scammers contacted users by phone, the average loss was $1,400 per user. This data highlights the importance of cross-sector collaboration in addressing growing digital fraud trends, along with the importance of mitigating the threat as close to the initiation of a call from a “scam center” as possible.

It is imperative to encourage the telecom industry, the social media industry and Big Tech platforms to participate in partnership with the banking industry to help address the scams and social engineering threats facing American consumers.

b) Enabling and empowering information and intelligence sharing

Sharing of intelligence, fraud-related data and key indicators of fraud plays a crucial role in reducing fraud by facilitating the exchange of relevant information among different entities, such as government agencies, financial institutions, businesses and law enforcement. This collaborative approach enhances the ability to identify, prevent and respond to fraudulent activities more effectively.

An example of effective efforts to improve collaboration is the Bank Policy Institutes | BITS Three-Pillar Strategy on Fraud Intelligence, which has established a three-pillar strategy to advance fraud sharing across the industry. The objective of this initiative is to enhance the financial industry's fraud management capabilities through the strategic development of three key pillars. The purpose of this effort is built around:

1) **Fraud Data Sharing**: Near-real-time fraud information sharing of account and transaction data associated with bad actors and/or fraudulent accounts.
2) **Fraud Intelligence Sharing**: Industry-wide timely sharing of fraud types, trends and major changes in fraud tactics – at scale - from an authoritative source
3) **Law Enforcement Collaboration**: Aggregation, analysis and packaging of cases and coordination with law enforcement against large-scale or organized fraud actors

This strategy aims to create a resilient, integrated and effective strategy for managing and preventing financial fraud. This strategy includes engagement with BPI's member banks, the ABA, the FS-ISAC, Early Warning Services (EWS) and others to deliver upon this strategy. Many elements of the strategy are underway with pilots beginning in 2024 including data sharing through the ABA and improved fraud intelligence sharing through FS-ISAC.

Here's how intelligence sharing can contribute to fraud reduction:

- **Early Detection of Fraud Patterns:** Sharing intelligence enables organizations to pool information on emerging fraud patterns, techniques and tactics. This collective knowledge helps in the early detection of new and evolving fraud schemes, allowing entities to proactively implement preventive measures.
- **Real-Time Alerts and Notifications**: By sharing intelligence in real-time, organizations can quickly alert others about potential threats or ongoing fraudulent activities. This rapid exchange of information enables entities to take immediate preventive actions to stop fraud attempts.
- **Information Fusion and Analysis:** Intelligence sharing helps in aggregating and analyzing diverse datasets from various sources. The fusion of information allows for a more holistic view of fraudulent activities and helps in identifying patterns and trends that may not be apparent when analyzing individual datasets in isolation.
- **Enhanced Investigation Capabilities:** Bi-directional sharing of intelligence provides between law enforcement agencies and banks, inclusive of more comprehensive information to conduct investigations. This can lead to the identification and apprehension of individuals or groups involved in fraudulent activities.
- **Fraud Prevention and Mitigation Strategies:** Collective intelligence enables organizations to develop and implement more effective fraud prevention and mitigation strategies. This can include the deployment of advanced technologies, enhanced authentication methods and targeted interventions to address specific fraud threats.

The Committee could pursue the following to help enhance fraud collaboration in sharing:

- **Encourage Regulatory Support:** Governments and regulatory bodies can play a role in facilitating intelligence sharing by establishing frameworks, standards and incentives for organizations to collaborate in the fight against fraud. Clear regulatory guidance can encourage responsible information sharing practices.
- **Promote Cross-Sector Collaboration:** Intelligence sharing fosters collaboration between different sectors, such as finance, retail, healthcare and telecommunications. Fraudsters often target multiple industries, and collaboration allows for a more comprehensive understanding of cross-industry fraud trends.
- **Educational Initiatives:** Promote education and awareness initiatives by encouraging organizations to actively participate in intelligence sharing. Understanding the benefits of

collaboration and the collective effect on fraud reduction can incentivize more entities to share relevant information.

- **Promote Global Collaboration Against Cybercrime:** In the case of digital fraud, international intelligence sharing is essential. Cybercriminals operate across borders, and global collaboration allows for a coordinated response to cyber threats, improving the chances of apprehending cybercriminals and dismantling criminal networks.

c) Persistent and Coordinated Customer Education

Equipping consumers and businesses with the knowledge to recognize scams is pivotal and in many ways the true first line of defense. Banks have consistently focused on educating their customers about the evolving fraud landscape and the importance of vigilance. This work, often done with other organizations such as AARP but could still benefit from partnerships with the public sector to reach an even larger audience. Collaborative private-sector education efforts include providing information on common fraud schemes, safe online practices and guidance on recognizing suspicious activities.

The public sector has also established a variety of education efforts on scams in recent years, which provide helpful educational materials and resources for consumers, but are coming from several sources and through assorted channels, thus not effectively reaching enough individuals to make a significant impact. Government-led messages have proven effective ways to inform customers on many national issues, an example includes the UK's Stop. Think Fraud Campaign, aimed at keeping scams and fraud top of mind for the customer to ensure they are aware. We believe it would be much more effective to leverage government resources to drive a central government-led national public awareness campaign. By raising public awareness and promoting a collective sense of responsibility in the fight against fraud, banks and regulatory bodies can better shield the financial ecosystem from the threats posed by sophisticated fraudsters by reducing volumes and enhancing positive effects of all other preventative actions.

Governments, agencies, trade organizations, telcos, social networks and banks should collaborate to provide consistent and persistent education and awareness programs to help customers protect themselves. By raising public awareness and promoting collective responsibility in the fight against fraud, banks and regulatory bodies can better shield the financial ecosystem from threats. The Committee should find ways to provide a framework for effective messaging to customers that can be easily applied at national levels.

B. Recommendation: Multi-Factor Authentication and Industry Standard Authentication

Embracing strong phishing-resistant authentication is a critical path in combatting digital fraud. A key enabler of digital fraud is the fact that many accounts outside of the banking system are still protected by a single-factor password.

FIDO, which stands for Fast Identity Online, is an open standard designed to address the challenges of traditional password-based authentication systems and enhance online security at the international level. FIDO aims to provide a more secure and user-friendly authentication experience by introducing stronger, multi-factor authentication methods that reduce reliance on passwords alone. The FIDO Alliance, a consortium of companies and organizations, develops and promotes these standards.

FIDO authentication uses standard public key cryptography techniques to provide phishing-resistant authentication. During registration with an online service, the user's client device creates a new cryptographic key pair that is bound to the web service domain. The device retains the private key and registers the public key with the online service. These cryptographic key pairs, called passkeys, are unique to every online service. Unlike passwords, passkeys are resistant to phishing, are always strong and are designed so that there are no "challenge questions."

The use of FIDO standard authentication can help to reduce fraud in several ways, including:

- **Reduced Reliance on Passwords:** FIDO aims to eliminate or minimize the dependence on traditional passwords, which are susceptible to various attacks such as phishing, brute force and credential stuffing.
- **Multi-Factor Authentication (MFA):** FIDO promotes the use of multi-factor authentication, combining something the user knows (password) with something they have (physical security key or biometric data). This significantly enhances the security of the authentication process.
- **Phishing Resistance:** Since FIDO implementations often involve cryptographic keys or biometric data stored locally on a user's device, phishing attacks become more challenging for fraudsters. Even if login credentials are captured through a phishing attempt, they are useless without the corresponding physical token or biometric data.
- **Device-to-Device Communication:** FIDO allows for secure communication between the user's device and the service provider, reducing the risk of man-in-the-middle attacks. Public-key cryptography is commonly used to secure these communications.
- **Privacy Protection:** FIDO protocols are designed with privacy in mind. User biometric data or authentication secrets are typically stored and processed locally on the user's device, reducing the risk of centralized breaches.
- **Interoperability:** FIDO standards are designed to be interoperable across various devices and platforms, allowing for a consistent and user-friendly authentication experience.

By addressing the vulnerabilities associated with traditional password-based systems, FIDO helps organizations enhance the security of user authentication processes, reducing the risk of unauthorized access and fraud. As more websites and services adopt FIDO standards, users can benefit from a more secure and convenient authentication experience across different online platforms.

MFA should be used by all banks and core industries such as Telcom and social networks, however, finding the right balance of customer experience and security is key in delivering a true strong but usable authentication experience for a customer. FIDO standards help enable this. The Committee should explore ways to enable standardized authentication approaches, like FIDO.

V. Concluding Statements

The Bank Policy Institute appreciates the opportunity to comment on this discussion paper. We believe that efforts to combat and understand how fraud is executed in a digital channel are imperative to effectively manage the issue and protect customers. Digital fraud is a complex and far-reaching issue, our recommendations and comments for this discussion paper are intended to ensure that the full depth and breadth of digital fraud is properly understood. This will enable a clear understanding, reduce duplicate work in categorization, and help to identify the right areas the Committee can focus on for

helping to address the issue and ultimately protect customers. We stand willing to join, participate and lead on joint initiatives that may arise in the next steps.

* * * * *

Respectfully submitted,

Gregory Williamson

Greg Williamson
Senior Vice President, Fraud Reduction
Bank Policy Institute