CBA Response to Basel Committee on Banking Supervision's Discussion Paper on Digital Fraud

1. Introduction

The Canadian Bankers' Association (CBA) is the voice of more than 60 domestic and foreign banks that help drive Canada's economic growth and prosperity. The CBA advocates for public policies that contribute to a sound, thriving banking system to ensure Canadians can succeed in their financial goals. We appreciate the opportunity to provide this submission to the Basel Committee on Banking Supervision (Committee) on its discussion paper titled 'Digital Fraud and Banking: Supervisory and Financial Stability Implications' (Discussion Paper).

Digital fraud has seen one of the sharpest increases among all fraud vectors during the last 24 months in Canada resulting in elevated financial losses for banks. Key drivers of this sharp increase include the pandemic-driven migration of many banking activities to digital channels, the rapid advances and public availability of advanced technologies like sophisticated Artificial Intelligence tools, an uptick in the frequency and scale of data breaches, ease in access to compromised digital credentials online for use by fraudsters, and growth in digitally-enabled fraud originating outside Canada. As a result, banks in Canada have experienced a significant increase in attempted digital fraud year over year in 2023. The Committee's Discussion paper is very timely, and the CBA commends the Committee for undertaking work on this important subject.

2. Executive Summary

Fraud today is predominantly digital with more products and services moving into the digital space. With advances in technology, new channels for perpetuating digital fraud continue to emerge. Banks in Canada are leaders in managing this risk and have invested heavily to protect the financial system and the personal information of their customers.

However, given the evolving nature of digital risk, it is important to recognize that while digital fraud may start online, it can materialize with customers physically interacting with their bank. Further, events such as a pandemic can amplify digital fraud. On a related note, it is important to distinguish between fraud and cases where customers are deceived and initiate transactions as the customer liability in the two scenarios should be assessed very differently.

It is also vital that all key stakeholders – banks, law enforcement agencies, government authorities, regulators, and cross-sectoral partners, especially telecommunications firms, payment processors, and retailers work together to help mitigate fraud and make customers and individuals aware of how to detect and protect against digital fraud. There is enormous potential for data sharing and the Committee should actively promote data sharing between the various participants of the financial services ecosystem, though this must be done in a way that safeguards privacy/protection of personal information and security.

3. Digital Fraud: Overarching Considerations

Before responding to the questions posed by the Committee in the Discussion Paper, the CBA wishes to draw attention to some overarching considerations in the context of digital fraud.

As a general observation, the CBA noted that the language in the Discussion Paper was focused on payments made using a debit or credit card. The inclusion of electronic funds transfers and real-time payments in the Discussion Paper will help provide a forward-looking view of the channels being exploited to commit digital fraud.

I. The Current Definition of Digital Fraud is Limiting

While we appreciate that the definition of digital fraud can vary based on jurisdiction and that the Committee has sought to define "digital fraud" in the context of the banking system, we suggest that the definition of "digital fraud" should encompass other fraud vectors. The first bullet under the sub-heading 'Key Points' in Section 1 of the Discussion Paper notes that digital fraud "*encompasses activities that are committed remotely and/or virtually*." This characterization is unnecessarily limiting given the proliferation of digital authentication methods available within retail branches (SMS OTP, Push to App, etc.) and other "digital" fraud vectors that involve physical branch access (ATM tap rather than card read, etc.).

Further, while digital fraud may start online, it can materialize with customers physically interacting with their banks. An example would be romance scams where the fraudster uses online methods to engage with a customer and persuades the customer to visit a branch to initiate a wire payment to the fraudster. Another example would be stolen identities that are bought on the web and then used to open accounts at bank branches with those identities.

We suggest that the Committee clarify that the comingling of in-person activities with remote/virtual activities does not necessarily preclude an overall case from still being classified as digital fraud. Additionally, while banks have internal fraud controls in place, it may be worthwhile to recognize the role internal fraud can play in amplifying digital fraud.

II. Proper Allocation of Risks

There is a need for the Discussion Paper to distinguish between unauthorized transactions and digital scams.

Generally speaking, Canadian customers are not liable for unauthorized transactions when dealing with their bank (subject to reasonable limitations - for example, if the customer demonstrated gross negligence in safeguarding their personal authentication information). Liability protection is provided to banking customers based on the type of the transaction. For example, many banks in Canada provide online security guarantees where the bank will reimburse their customer if a customer suffers financial loss due to unauthorized activity while using their online banking portal or mobile banking. Credit card networks also offer zero liability policies where customers (including customers who use bank-issued credit cards) are not held liable for certain types of unauthorized use. There is also federal consumer protection legislation in place in Canada that applies to banks that caps customer liability for certain types of unauthorized use of a credit card (similar protections exist in some Canadian provincial/territorial customer protection legislation). Liability protections are also in place for customers making purchases online using their debit card under Interac's Zero Liability Policy. Further, CBA member banks have publicly committed to applying the principles and provisions of the Canadian Code of Practice for Consumer Debit Card Services as applicable to

online payment items in respect of customer deposit accounts. Compliance with public commitments is overseen by the Financial Consumer Agency of Canada (FCAC). Similarly, the FCAC oversees compliance with federal legislation (i.e., the *Bank Act* and supporting Financial Consumer Protection Framework Regulations).

Banks have both legal and contractual obligations to honor their customers' instructions and act on them so long as the customer has sufficient funds available, either on credit in their account or by borrowing them. When banks carry out their customers' instructions, they are acting as their customer's mandatory. They do not become an insurer of the transaction, and unless exceptional circumstances are involved, banks are entitled to treat their customers' mandates on their face value. It is a recognized principle in banking law that financial institutions should not unduly interfere in the internal affairs of their customers. Therefore, it is important to distinguish unauthorized transactions (e.g., account takeover) from cases where customers are deceived and initiate transactions (e.g., when they fall for a scam) as a result. While the CBA and its member banks educate customers about how to protect against scams and bank staff are trained to pay attention to unusual transactions, customers are in the best position to assess whether an interaction poses fraud risks. Customers are held liable in Canada for financial losses if they initiated the transaction after falling prey to such a scam (though on an exception basis, banks may provide some financial relief). A change in the liability model could, among other negative unintended consequences, give rise to risky customer behaviour. Other negative unintended consequences could include greater processing times (on account of verification of greater number of transactions) when major retail payment systems, including Canada's, have or are planning to move to faster or real-time payments, and higher transaction costs. In this regard, we wish to highlight that Banks in Australia have recently decided to delay instant money transactions in a bid to combat the explosion of scams[1].

Therefore, the CBA recommends that the Committee draw a distinction between unauthorized transactions and scams in the context of discussing risks associated with digital fraud.

III. Role of the Customer

The implementation of Multi-Factor Authentication (MFA) technology and the use of voluntary notifications (e.g., receiving email/text when a bill is paid from the bank account or when a purchase is made using a debit/credit card, etc.) has allowed customers to play an increasingly vital role in the prevention of digital fraud. This practice helps to ensure that transactions are genuine.

While banks make MFA and notifications available and strongly encourage their use, customers need to opt into the full range of these banking features to enable banks to effectively investigate and manage fraud alerts more effectively.

The CBA urges the Committee to acknowledge the customer's role and participation in combatting digital fraud.

IV. Additional Channels for Digital Fraud

The CBA requests that security breaches at a merchant or at an aggregator be identified in the Discussion Paper as an important contributor to Digital Fraud.

[1] Banks to delay instant money transactions in bid to combat explosion of scams as government prepares major crackdown | Sky News Australia.

Additionally, the risk of digital fraud from a consumer perspective remains elevated as unregulated and underregulated entities continue to take on more bank-like functions and offer services such as open banking. The CBA requests that the Discussion Paper discuss the risks associated with the presence of a large number of unregulated and underregulated entities offering financial services.

V. Banks' Track Record in Managing Cyber Security

Digital fraud is committed by bad actors using the latest cyber technologies. Banks in Canada are leaders in cyber security risk management and have invested heavily to protect the financial system and the personal information of their customers from cyber threats.

Over the past decade (2012-2022), Canadian banks have invested approximately $115 billion on technology, which includes technology dedicated to security measures. In fact, cyber security measures and procedures are part of the banks' overall security approach that includes teams of security experts that monitor transactions, prevent and detect fraud and maintain security of customer accounts.

As leaders in the prevention and detection of security threats, banks in Canada continue to provide active leadership to improve the resiliency of the financial sector against cyber threats, in partnership with key stakeholders within the government and law enforcement.

The banking sector in Canada continues to work with the federal government and the Canadian Centre for Cyber Security to successfully implement the National Cyber Security Strategy with the common goal of creating a more resilient, safer cyber environment for Canadian citizens and businesses.

The CBA requests that the Committee explicitly recognize the banks' efforts in managing cyber security despite the sudden increased adoption of digital banking.

VI. Customer Education: Need for greater participation by other stakeholders.

Supporting greater participation of other stakeholders such as telecommunication companies, social media companies, merchants, card networks, payment processors, credit bureaus, and governments is key[2]. While banks continue to educate their customers, relying solely on banks to educate customers and create awareness may be insufficient as digital fraud trends/attack vectors are pervasive across the industry and involve other industry partners.

It will take a coordinated effort by all key stakeholders to effectively educate customers and prevent and mitigate digital fraud.

[2] The CBA also recommends that the Committee advocates for governments to develop digital credential ecosystems as they could aid in combatting digital fraud.

Discussion Paper Questions

4. Do you agree with the features and categories of digital fraud?

I. Features of Digital Fraud

a) Identify primary fraud prevention responsibility and accountability in scenarios where banks' play an indirect role.

Based on customer behaviour and preferences, social media channels are becoming increasingly popular as a means of banks' communication to customers (i.e., promotional campaigns, etc.) in addition to traditional electronic communications channels, such as emails and text messages. Frequently, these communications include web links to banks' or third-party websites, which present an additional opportunity for fraudsters to impersonate banks' legitimate communications, insert fraudulent weblinks, leading to a theft of a customer's personally identifiable and financial information, payment card data, and online banking log on credentials. Customers become accustomed to seeing legitimate banks' communications through these additional channels and become more susceptible to fraud scams. While banks monitor for instances of fraud using third-party platforms (e.g. when a fraudster is impersonating a bank), it is important in the customer's interest to identify and regulate non-bank actors whose platforms serve as the platform for propagating such fraud.

II. Categories of Digital Fraud

a) Feedback on existing categories

i. Need for greater clarity between Category 2 (Unauthorized payment transaction) and Category 3 (Digital Fraud Related to Bank Customers' Other Banking Products).

Category 2: Digital fraud related to online payment instruments: manipulation of the payer to issue a payment order is described as follows:

"Digital fraud activity under this category comprises fraudulent transactions made as a result of the payer being manipulated by the fraudster to issue a payment order or to give the payment service provider the instruction, in good faith, to a payment account it believes belongs to a legitimate payee. For example, this includes such activity conducted through social engineering techniques (e.g. phishing emails, text message or phone calls), impersonation of the bank (e.g. spoofing) or any other trusted third party."

Category 3: Digital Fraud Related to Bank Customers' Other Banking Products has been described to include "*fraudulent activities on other banking products, for instance when customers are manipulated into investing in fake saving products or taking on fake credit products."*

Category 2 is product agnostic and therefore seems to be inclusive of the scenario that is described under Category 3. The CBA requests the Committee to clarify, by way of example, the fraudulent activities that would fall under Category 3.

ii. Inconsistency between the Description of Category 4 and the Definition of Digital Fraud.

Category 4 description provides:

"4. Digital fraud related to the bank through customers' data or banks' systems.

A fourth category of digital fraud targets the bank itself through misuse of customers' data or banks' systems. For instance, it can be the opening of bank accounts and/or applying for credit cards using stolen identities (e.g. bought on the dark web) or false identities, and the use of these accounts and/or cards as a relay in money laundering circuits, to receive fraudulent transactions, use associated payment instruments or subscribe to loans, etc. 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."

This description seems to be referring to two scenarios i.e. True Name Fraud/Synthetic ID Fraud and an event related to the compromise of the banks' systems and employees' accesses which is more aligned with a cyber incident/attack. However, this description appears to be inconsistent with the description of digital fraud in the sub-section titled 'Defining digital fraud' of Section 1 wherein digital fraud has been described to be "***related to but different from***, *operational risk/resilience, cyber risk and/or social engineering."* (Emphasis added).

iii. Update the Description of Categories 2 and 3 to accurately reflect the distinction between Digital Fraud and Social Engineering.

Sub-section titled 'Defining digital fraud' of Section 1 describes digital fraud as "***related to but different from***, *operational risk/resilience, cyber risk and/****or social engineering****."* (Emphasis added)

Under Box A, social engineering has been defined as "*A general term* ***for trying to deceive people into revealing information or performing certain actions****" (FSB, 2023). Some aspects of social engineering are a tool for digital fraud, while other aspects relate to deceptions that are beyond digital fraud".* (Emphasis added)

Digital Fraud Category 2 named *"Digital fraud related to online payment instruments:* ***manipulation of the payer*** *to issue a payment order"* refers to digital frauds involving manipulation by the fraudster.

This category of fraud appears to be covered squarely under the definition of social engineering discussed above. Further, given that digital fraud "***…is related, but different from …. Social engineering***", there appears to be an inconsistency within the document

around the treatment of such kind of fraud. The same applies even with respect to Category 3.

The CBA requests that the Committee reconsider the descriptions of Categories 2 and 3 to accurately reflect the distinction that the Committee is seeking to make between Digital Fraud and Social Engineering.

b) Additional proposed categories

We recommend that the following categories be expressly recognized by the Committee:

i. Authorized Push Payment (APP) fraud

APP fraud is a growing vector within digital fraud. Common examples include job scams, cryptocurrency scams, romance scams, investment scams, etc.

APP fraud saw a sharp rise during the pandemic and is typically perpetrated by scamming a customer to make a monetary transfer of funds to a fraudster impersonating a legitimate entity. As banks get better at detecting out-of-pattern activity indicative of third-party fraud (through the use of controls such as multi-factor authentication and behavioural biometrics), fraudsters will shift to focus on the customer (leveraging new tools such as generative AI).

As noted above, these types of fraud, where the customer had *intended* to pay the payee, and the bank is properly acting on the instruction of its customer, need to be distinguished from unauthorized transactions and other types of digital fraud.

ii. Friendly or First-Person Fraud

Frauds where a cardholder tries to fraudulently chargeback. This may not affect issuers so much as card schemes or other parties, depending on the implementation of the chargeback.

iii. Identity Theft

This type of fraud is especially concerning due to the prevalence of data breaches across a wide range of organizations that store customer's personal information and the digital options for opening a new account.

iv. Emerging Digital Fraud

Given the rapid technological advancements especially in the field of Artificial Intelligence, we recommend that the Discussion Paper acknowledge the increasing usage of sophisticated AI-driven mechanisms to perpetrate fraud on banking customers by fraudsters which may not explicitly be covered in the categories acknowledged in the Discussion Paper. This risk is expected to amplify with the launch of Real-Time Payments and Open Banking in Canada.

v. Leverage Existing Frameworks for Fraud Categorization

In addition to the categories proposed above, there are additional categories of digital fraud listed under the fraud classification model 'FraudClassifier[SM]'[3] developed by the

[3] https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/fraudclassifier-model/.

Federal Reserve which is well known to fraud professionals in both the US and Canada. As the digital fraud landscape continues to evolve, it will be helpful for the Committee to leverage this tool for identifying additional categories of digital fraud.

5. Are there additional financial stability and/or prudential transmission channels from digital fraud to the banking system?

Given the rapid growth and sophistication of digital fraud schemes, detection of the same can come at the expense of increased false positives. This in turn often leads to the abandonment of sales for service providers, loss of revenue for banks, and an impact on customer experience. Mitigating this requires the allocation of capital that would otherwise be spent on innovation.

Further, digital fraud schemes can pose greater risks for real-time payments. This could result in customers and banks needing to take additional measures to screen for potentially fraudulent transactions.

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

I. Additional Data Sources

The following channels should be explored for gathering incremental digital fraud data:

a) **Payment processors and networks:** Payment processors and networks, including, Visa, MasterCard, American Express, Swift, Symcor, Zelle, FIS, Fiserv, NACHA, and Interac (Canadian Interbank Network) are a rich source of data for data on electronic payments fraud.

b) **Credit Bureau Agencies**: Credit bureau agencies (such as Equifax and TransUnion in Canada) may be able to provide data on fraudulent accounts/product openings where stolen/synthetic identities are involved.

c) **Third-Party Reports and Research:** We recommend the Committee consider research available through third-party vendors. Some recommendations are listed in Appendix 1.

II. Future Data Sources

a) Payments Canada is developing a fraud prevention framework in support of the Real-Time Rail (RTR) payment infrastructure. Within the scope of RTR Release 1, Payments Canada mandates that all RTR members submit monthly fraud reports. This data could be another potential source of fraud data from Canada for the Committee in the future.

b) We expect the Committee to be acquainted with the upcoming information-sharing platform to be launched in the United States later this year by the American Bankers Association to help fight fraud.

III. Caveat for Existing Data Source

With respect to the Canadian Anti-Fraud Centre (CAFC) data referenced in the Discussion Paper, we would like to draw attention to the fact that the collection of data by CAFC is dependent on reporting by customers.

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

I. Recommend Enhanced Cybersecurity Standards for Non-Banking Participants

The Committee should consider drafting recommendations for regulators proposing cyber security standards for non-bank participants in the banking ecosystem, such as e-commerce websites (e.g.: stronger secure browsing protocols for merchant portals where customers make financial purchases of goods), telcos (e.g.: usage of SMS text messages to deliver OTP codes), etc. This will ensure the balancing of risk to protect the banking ecosystem.

II. Develop additional data sources for assessing digital fraud.

a) **Increased Domestic Network Intelligence Sharing:** While there is increasing importance and investments within banks on fraud management, including digital fraud, the Committee should consider proposing setting up a network intelligence sharing mechanism amongst banks to increase inter-bank information sharing to reduce bank-hopping by fraudsters that typically amplifies the impact of a digital fraud event in a country's financial system. In Canada, early discussions are underway through Payments Canada to establish such a mechanism, though it is currently focused solely on establishing the framework to support the rollout of Real-Time Payments in Canada. The Committee should consider making recommendations on information that can be safely shared within banks as well as a framework for information sharing keeping in mind competition law, privacy and cyber security considerations.

b) **Promote cross-border sharing of data**: Given that bad actors are often based outside the jurisdiction in which they perpetuate fraud and that such actors often target banks/customers in multiple jurisdictions, the Committee should encourage greater cross-border cooperation for sharing of fraud data which will go a long way in preventing and mitigating digital fraud.

c) **Data sharing with partners:** The Committee should encourage sharing of fraud data between merchants, networks, credit card interchange, cheque systems, electronic payment systems, etc.

d) **Data breach reporting for customer information sold online:** There has been a rapid increase in data breaches observed annually, on many occasions containing personally identifiable information and financial information. This information is often sold online through dark web forums. Banks at times have limited information on the impacted population, hence, limited ability to put enhanced controls in place if this information is reused to commit fraud.

We recommend that the Committee propose mechanisms through which this information could be shared with banks to detect fraud through the reuse of compromised information. This will help prevent new accounts opened using compromised/stolen information without the real customer's knowledge as well as monetary transfers made using this information. An option for consideration would be sharing information with credit bureaus who in turn can share this information through fraud markers to banks, enabling fraud monitoring.

e) **Data sharing by social media networks:** Some jurisdictions are starting to track the intersection of social media with digital fraud, and the Committee should consider emphasizing the materiality of social media platforms on the future state of payments. Social media platforms are key enablers of ubiquitous commerce, their co-mingling of content from known entities with advertisements and other solicitations tends to reduce customer vigilance, and by their nature, social media platforms make customers accessible to perpetrators of fraud, deception, and extortion at a massive scale.

f) **Data sharing by Internet Corporation for Assigned Names and Numbers (ICANN):** The Committee could facilitate data sharing by ICANN on domain names that are associated with at least one of the four kinds of security threats: phishing, malware distribution, botnet command-and-control, and spam.

The CBA appreciates that proper mechanisms will be required to be in place to facilitate the sharing of information discussed above and we would be pleased to be consulted by the Committee in that regard.

III. Urge internet service providers and telcos to strengthen controls.

A key mechanism used by fraudsters to commit digital fraud is the use of telecom services, such as SMS text messages, VoIP calls, or emails often impersonating a bank, to steal customer information through sophisticated phishing schemes to deplete a customer's financial assets. We recommend the committee acknowledge this growing trend and urge stronger controls for internet service providers and telcos to filter ‘known bad’ traffic and prevent the usage of their service to commit fraud.

IV. Recommend greater regulatory oversight on non-banks.

The Committee should consider recommending greater regulatory oversight over non-bank actors that pose a higher risk and encourage regulatory oversight based on the ‘same activity, same regulation’ approach.

V. Recommend adequate resourcing of law enforcement agencies.

Law enforcement agencies have a vital role to play in the effective detection and suppression of digital fraud. We request that the Committee encourage governments to allocate adequate resources to support industry efforts around managing digital fraud risk.

VI. Correlation with data across other risk domains

The Committee should consider providing guidance on reviewing the data points across other risk domains such as privacy, cyber security attacks, data breaches, AML, and financial crimes to assess their correlation with digital fraud.

VII. Customer Education and Advocacy Programs

Given the rapid increase in digital fraud, the Committee should consider leveraging the Basel platform to influence key authorities (e.g.: governments, regulators, etc.) to acknowledge and complement customer education and advocacy programs offered by banks to educate the broader population against digital fraud.

Appendix 1
Third-Party Reports and Research

1. 2023 Global eCommerce and Payments Fraud Report: https://www.cybersource.com/content/dam/documents/campaign/fraud-report/global-fraud-report-2023-en.pdf
2. Lexis Nexus True Cost of Fraud in Financial Services Report: https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study
3. Lexus Nexus Global State of Fraud and Identity Report: https://risk.lexisnexis.com/global/en/insights-resources/research/global-state-of-fraud-and-identity
4. IBM Cost of Data Breach: https://canada.newsroom.ibm.com/2023-IBM-Cost-of-a-Data-Breach-Report-Canadian-businesses-are-being-hit-hard
5. PwC Global Economic Crime and Fraud Survey: https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html
6. Aite Novarica Fraud Trends for 2023 and Beyond: https://www.datavisor.com/intelligence-center/reports/aite-trends-in-fraud-for-2023-and-beyond/
7. Experian 2022 Global Identity and Fraud Report: https://www.experian.com/blogs/insights/experians-2022-global-identity-fraud-report/
8. IBM Security X-Force Threat Intelligence Index 2023: https://www.ibm.com/reports/threat-intelligence
9. Using AI and collaboration to prevent consumer payment scams: https://b2b.mastercard.com/news-and-insights/report/fincrime-using-ai-and-collaboration-to-prevent-consumer-payment-scams/
10. TransUnion Report on Digital Fraud Attempts in Canada: https://newsroom.transunion.ca/digital-fraud-attempts-in-canada-spike-189-from-pre-pandemic-reveals-new-transunion-report/
11. Nasdaq Verafin 2024Global Financial Crime Report; Nasdaq Verafin 2024 Global Financial Crime Report | Nasdaq