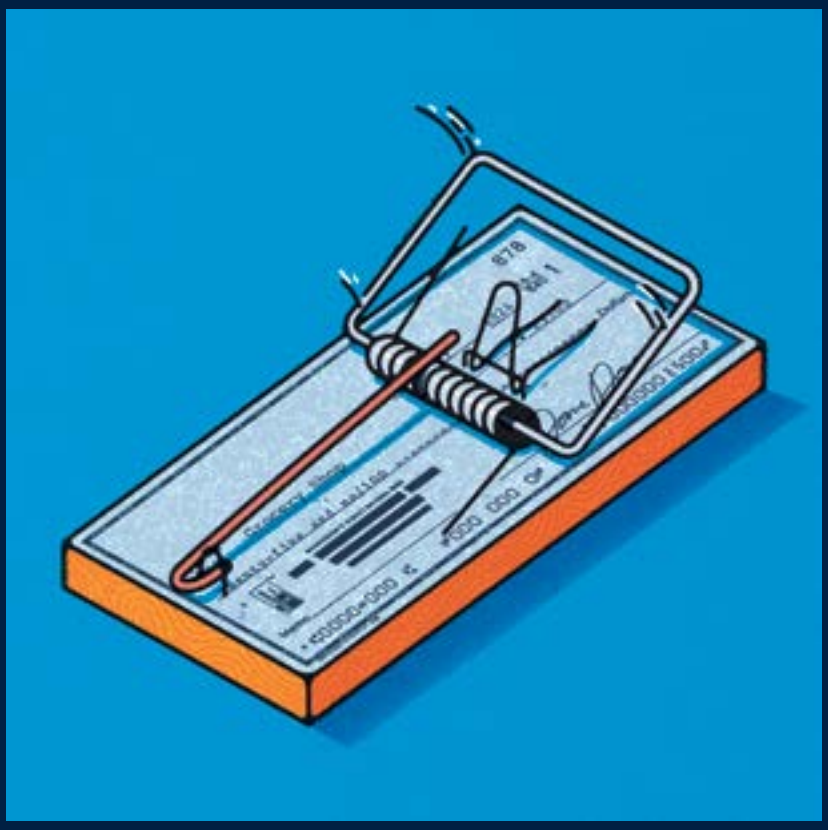
BNY

Fighting to Stay Ahead of PAYMENTS FRAUD

BY SADHBH CLOONAN



BY THE NUMBERS

$429 BILLION

The cost of payments fraud in 2023 in the retail sector alone[1]

80%

Of organizations experienced attempted or actual check-related payment fraud in 2023[2]

63%

Of organizations experienced business email compromise in 2023[3]

$25 MILLION

Amount a finance worker was duped into sending to a fraudster through deepfake AI imitation[4]

SOURCES:

1. Research from the Centre for Economics and Business Research
2. Association for Financial Professionals, 2024 AFP Payments Fraud and Control Survey Report
3. Association for Financial Professionals, 2024 AFP Payments Fraud and Control Survey Report
4. CNN World

The battle against payment fraud is intensifying. From emerging trends like the growth of scams inducing account holders to authorize payments, to the scaling-up of pervasive AI-powered attacks, the financial ecosystem is under siege. Financial institutions are fighting back, but with many customers still writing checks and fraud tactics ever evolving, banks have their work cut out for them.

BY SADHBH CLOONAN

Despite what Hollywood movies like "Catch Me If You Can" would have you believe, the business of tackling payments fraudsters seldom involves high-octane globetrotting adventures. Rather than frantic chases across airport terminals, it is a methodical business of detecting illicit activity, correcting weaknesses, and the decidedly unglamorous work of remaining ever vigilant to thwart the next attempted attack.

Fraud prevention is a largely thankless but nonetheless immensely important task. The cost of payments fraud in 2023 in the retail sector alone was $429 billion, according to research from the Centre for Economics and Business Research. When the overall global institutional payments ecosystem is taken into account, the annual cost of payments fraud likely stretches into the trillions of dollars.

In the realm of payments, the prevalence of fraudulent transactions and the net value of those illicit remittances continues to climb each year. A 2024 payments fraud survey by the Association for Financial Professionals (AFP) found fraudulent activity soared in 2023 relative to the previous year, with 80% of organizations reporting that they were victims of attempted or actual fraud in 2023 - an uptick of 15% from 2022.

Despite heightened awareness around fraud - November 17, 2024, marks the beginning of "International Fraud Awareness Week" - and rapidly improving detection and prevention tools, fraudsters are responding by deploying increasingly sophisticated techniques to find new and inventive entry points to exploit.

OLDEST TRICK IN THE BOOK

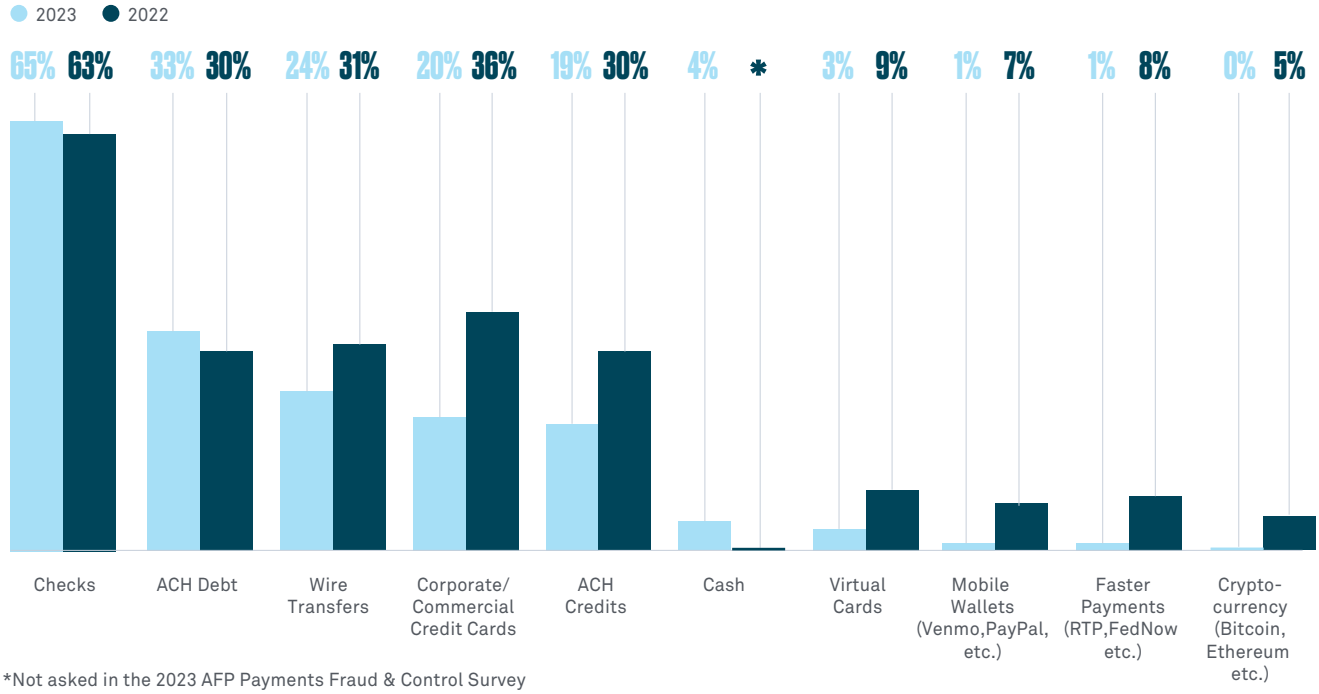
The rise in transaction fraud across financial services has often been linked to the development and rollout of real-time payments systems, with the misleading phrase "faster payments mean faster fraud" becoming commonplace. Focusing the discussion on the speed with which payments are completed risks missing the larger point, however.

"The focus on fraud prevention is more critical than ever, and especially in the dawn of faster payments, it's more prevalent today than we've seen before in the industry. From ACH payments to checks, there is a tremendous amount of fraud and we as an industry can - and should - do more," says Carl Slabicki, executive platform owner, Treasury Services at BNY.

The point is demonstrated in the AFP report, which reveals that of all U.S.

THE CHECK BOUNCED

Payment methods subject to attempted/actual payments fraud



*Not asked in the 2023 AFP Payments Fraud & Control Survey
Source: Association of Financial Professionals, Payments Fraud & Control Survey Report 2024

FIGURE 1

> "Everything old is new again - stealing checks out of a mailbox seems like an old-fashioned technique but it's a real and ongoing threat."
>
> **CARL SLABICKI, BNY**

payment methods, checks are the most susceptible to fraud, followed by ACH debits. In fact, real-time payment networks and faster payments were found to be the second-least likely forms of transaction to be targeted by fraudsters (see Figure 1).

That fraudulent checks remain the most prevalent form of payments fraud in the U.S. is not surprising. Slabicki explains that while we might imagine fraudsters to be using sophisticated technology to initiate attacks, they will resort to any means necessary, exploiting any weakness or vulnerability, no matter how basic. "Everything old is new again - stealing checks out of a mailbox seems like an old-fashioned technique but it's a real and ongoing threat," said Slabicki.

In fact, check fraud related to mail theft remains sufficiently rampant that in February 2023 the Financial Crimes Enforcement Network (FinCen) alerted financial institutions of fraud schemes targeting the United States Postal Service, which prompted the rollout of 12,000 new high security collection boxes and 14,000 electronic locks.

The volume of checks processed by the Federal Reserve declined 8.3% each year between 2018 and 2021, building on the existing 6.8% decline witnessed each year between 2000 and 2018, according to an April 2023 working paper from the Federal Reserve Bank of Atlanta. However, the customers and organizations who remain doggedly loyal to writing checks are increasingly vulnerable to being victims of fraud. FinCen statistics reveal that the number of suspicious activity reports (SARs) the agency receives pertaining to checks is increasing, in spite of declining check volume overall.

Despite rising fraud - and the rest of the world having largely phased out checks - over 70% of organizations in the U.S. do not have plans to discontinue check use, according to AFP. While support for checks remains high, Eric

Woodward, senior advisor at identity verification and fraud prevention company Socure, compares the inevitable obsolescence of checks with the demise of DVD rentals. "When Netflix phased out DVD rentals in favor of streaming people were up in arms, but now we can barely remember what a DVD is. As banks begin to end checks, I think we will see a similar phenomenon," he says.

DIGITAL FORTRESS?

Those that make the leap from the checkbook to digital payments are by no means free from the risk of fraud, however. A March 2024 Interpol assessment on global financial fraud highlighted how the increased adoption of technology is enabling organized crime groups to better target victims around the world.

In particular, the report noted that artificial intelligence (AI), large language models and cryptocurrencies are being combined with phishing and ransomware-as-a-service business models to create more sophisticated and professional fraud campaigns at relatively little cost and without the need for criminals to develop advanced technical skills.

"Today, our lives and our devices are increasingly interconnected - and that includes in the payments space. It means there are many more access points for fraudsters to exploit. This is what motivates us to innovate faster and smarter to protect our customers from emerging fraud threats with the latest AI technology," explains Rohit Chauhan, executive vice-president AI fraud solutions at Mastercard.

Through these access points fraudsters target customers to send payments, typically when they are distracted at work, or by using social engineering techniques to prey on emotions. The most prevalent form of attack is the business email compromise (BEC), where a criminal accesses a work email account to trick someone into transferring money. The U.S. Federal Bureau of Investigation received 21,832 BEC complaints in 2022, and in 2023 AFP reported 63% of organizations experienced BEC scams (see Figure 2).

AI and large-language models are creating new ways to defraud people, businesses and even governments. While AFP reports that only 1% of fraud attempts in 2023 were related to "deepfake" technology, this increased more than tenfold between 2022 and 2023, with North America and Asia-Pacific most affected.

AI is also reducing the barriers of entry for criminals. "Fraud-as-a-service" platforms like Fraud GPT - a criminal version of Chat GPT - are now available on the dark web. "This allows people without any fraud or technology experience to produce convincing phishing emails," explains Yuval Marco, general manager for enterprise fraud management at NICE Actimize. "But it also gets much worse: They can generate malware that can be deployed on different devices, and they can also easily create synthetic identities."

BUILDING A SOLID FRAUD DEFENSE

How are financial institutions responding to the plethora of methods criminals are using to perpetrate fraudulent transactions? For sender banks there are a number of steps that can help ensure a payment is legitimate. The first is for a bank to confirm that the payment instruction is a genuine request from a customer. Banks typically require customers to authenticate the request, by entering a one-time verification code, providing biometric verification, or answering a security question.

Second, banks check if a transaction falls within a customer's set parameters. For retail customers, this could be as simple as a daily transaction limit.

> "There is a new wave of AI imitation being used by criminals, and we are just at the beginning of trying to understand the responsible ways to insert it into our defenses."
>
> **IAN MITCHELL, MISSION OMEGA**

"All participants in the payment chain have a role to play, starting with the initiation of the transaction. But the institution on the receipt side might have the best opportunity of all to spot when it's a fraudulent transaction."

DEVON MARSH, NACHA

If the payment instruction passes the initial set of filters, the bank must validate that the beneficiary is legitimate using proprietary tools or network analytics. "We process the equivalent of the world's GDP every three days in our network, and we can use this transactional data to identify anomalies - and those anomalies could be fraudulent, or they could be operational errors," says Stephen Grainger, global head of data and services at Swift.

After these tests have been satisfied the payment could still be fraudulent - no validation service has 100% market reach so there are always gaps. The beneficiary account might be correct, but that doesn't tell the bank that that person isn't a scammer. This has become the payments industry's main pain point - and as fraud gets increasingly sophisticated, the harder this final verification step becomes.

Some progress is being made here. Nice Actimize has been using AI and machine learning to optimize transaction accuracy and has developed typology-based risk models that provide greater fraud detection than a transactional model.

"All participants in the payment chain have a role to play, starting with the initiation of the transaction," explains Devon Marsh, managing director of ACH network rules & risk management at ACH governing body Nacha. "But the institution on the receipt side might have the best opportunity of all to spot when it's a fraudulent transaction."

This is because most of the liability - and hence, the controls and protections on fraudulent payments - is with the sending bank. But the rise in induced payment fraud - also known as authorized payment fraud - has created a challenging situation for the sending bank. For example, a scammer sells fake tickets to 500 people and each buyer approves their payment via their bank's authentication controls because they believe it to be a legitimate transaction. The challenge is then when they turn to their bank to report the fraudulent activity, because, from the bank's perspective, each of the payments are correct and authorized.

However, at the receiving bank, the scammer's account will be receiving 500 payments for similar amounts with similar reference words. Many believe there is an opportunity here to mitigate fraud and pressure is mounting on receiving banks to do more - but how can the industry hold the bad actors accountable?

Nacha is one of the first movers in this space and is introducing new rules that require receiving institutions to address fraud through monitoring inbound payments. Effective March 2026, these rules will impose new requirements on receiving institutions, mandating them to put monitoring in place on all incoming credit transactions.

INFORMATION SHARING

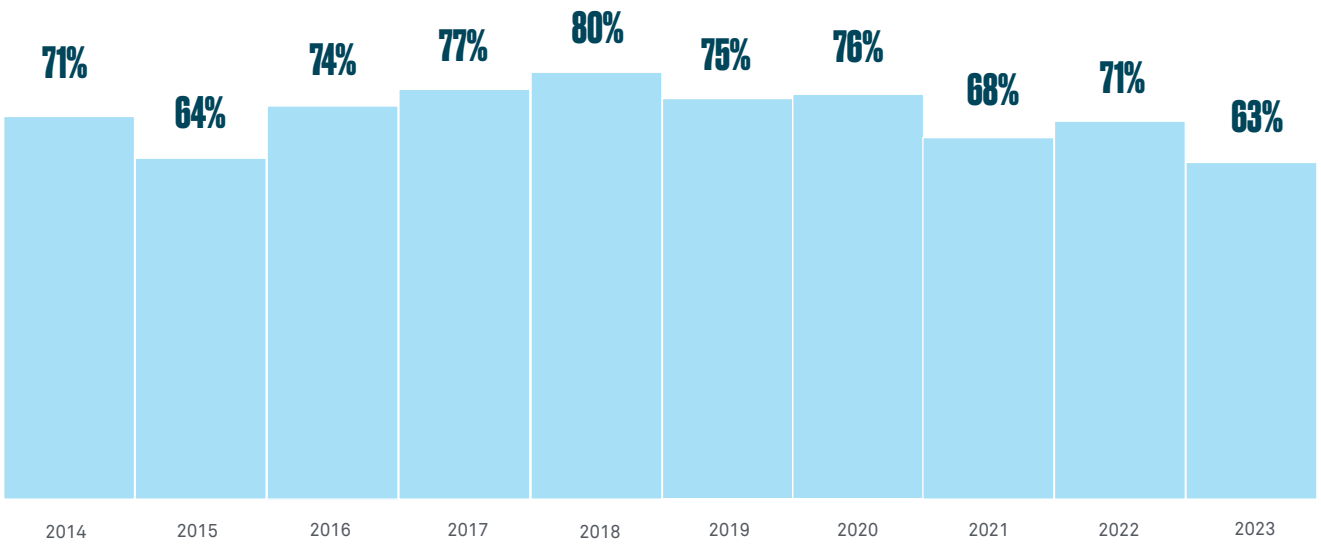
One way forward in the fight against payment fraud is increased information sharing in the industry - but there are both opportunities and challenges to consider.

Greater intelligence sharing would help models learn from more data points and better detect fraud - but there are rules around privacy laws that need to be considered. "We need to make sure how we're sharing data points and intelligence is beneficial to our customers," says David Pollino, global head of fraud prevention at BNY.

The ability of increased data points to thwart fraud attempts has

YOU'VE GOT MAIL

Percent of organizations that experienced business email compromise, 2014 - 2023



Source: Association of Financial Professionals, Payments Fraud and Control Survey Report 2024

FIGURE 2

been long proven, especially when combined with AI. For instance, Mastercard's Decision Intelligence Pro solution is reputed to be able to scan one trillion data points in less than 50 milliseconds and predict whether a transaction is likely to be genuine or not. By supercharging the algorithm and number of data points, fraud detection rates are boosted by 20% on average - but as high as 300% in some instances.

Elsewhere, Swift has been exploring how advanced AI can analyze anonymously shared data from different sources, ultimately aiming to enable financial institutions to exchange relevant information with strong privacy-preserving controls. The pilot program which was launched in May 2024, tests the use of secure data collaboration and federated learning technologies in collaboration with 10 leading financial institutions, including BNY.

The Federal Reserve is working to make information sharing easier and has established a working group to examine the mechanisms on how we share information.

CONCLUSION

Across the globe, organizations are making significant investments in payments trying to keep up with the ever-evolving threat of fraud. Those who haven't already made investments are grappling with old threats, while the rest are combatting the latest criminal tactics. Soon, all participants in the payments value chain will be contending with the next generation of fraud attacks, with all the potential threats that AI and quantum computing may present looming large on the horizon.

No matter the speed of these technological changes, the financial services industry will continue to defend both the physical and digital payment ecosystems and ensure they are trusted, safe and reliable for all who use them. "Fraudsters may be ahead of the curve, but we will be chasing closely behind in this never-ending game of cat and mouse," concludes Woodward.

Sadhbh Cloonan is a freelance writer based in London.

Questions or comments? Write to treasury@bny.com, or reach out to your relationship manager.

BNY.COM

BNY is the corporate brand of The Bank of New York Mellon Corporation and may be used to reference the corporation as a whole and/or its various subsidiaries generally. This material and any products and services may be issued or provided under various brand names of BNY in various countries by duly authorized and regulated subsidiaries, affiliates, and joint ventures of BNY, which may include any of those listed below: The Bank of New York Mellon, a banking corporation organized pursuant to the laws of the State of New York, whose registered office is at 240 Greenwich St, NY, NY 10286, USA. The Bank of New York Mellon is supervised and regulated by the New York State Department of Financial Services and the US Federal Reserve and is authorized by the Prudential Regulation Authority (PRA) (Firm Reference Number: 122467). In the UK, a number of services associated with BNY Wealth Management's Family Office Services - International are provided through The Bank of New York Mellon, London Branch. The Bank of New York Mellon also operates in the UK through its London branch (UK companies house number FC005522) at 160 Queen Victoria Street, London EC4V 4LA, and is subject to regulation by the Financial Conduct Authority (FCA) at 12 Endeavour Square, London, E20 1JN, UK and limited regulation by the PRA at The Bank of England, Threadneedle St, London, EC2R 8AH, UK. Details about the extent of our regulation by the PRA are available from us on request. Investment management services are offered through BNY Mellon Investment Management EMEA Limited, BNY Centre, 160 Queen Victoria Street, London EC4V 4LA, which is registered in England No. 1118580 and is authorised and regulated by the Financial Conduct Authority. Offshore trust and administration services are through BNY Mellon Trust Company (Cayman) Ltd. BNY Mellon Fund Services (Ireland) Designated Activity Company is registered with Company No 218007, having its registered office at One Dockland Central, Guild Street, IFSC, Dublin 1, Ireland. It is regulated by the Central Bank of Ireland. The Bank of New York Mellon operates in Germany through its Frankfurt am Main branch with registered office at FriedrichEbert-Anlage 49, 60327 Frankfurt am Main, Germany (Zweigstelle registered in Germany with Registration No. HRB12731). It is under the supervision of the German Central Bank and the Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Marie-Curie-Str. 24-28, 60439 Frankfurt, Germany) under BaFin-ID10100253. The Bank of New York Mellon SA/NV, a Belgian public limited liability company, with company number 0806.743.159, whose registered office is at Boulevard Anspachlaan 1, B-1000 Brussels, Belgium, authorised and regulated as a significant credit institution by the European Central Bank (ECB), under the prudential supervision of the National Bank of Belgium (NBB) and under the supervision of the Belgian Financial Services and Markets Authority (FSMA) for conduct of business rules, a subsidiary of The Bank of New York Mellon. The Bank of New York Mellon SA/NV operates in Ireland through its Dublin branch at Riverside II, Sir John Rogerson's Quay Grand Canal Dock, Dublin 2, D02KV60, Ireland and is registered with the Companies Registration Office in Ireland No. 907126 & with VAT No. IE 9578054E. The Bank of New York Mellon SA/NV, Dublin Branch is subject to additional regulation by the Central Bank of Ireland for Depository Services and for conduct of business rules. The Bank of New York Mellon SA/NV operates in Germany as The Bank of New York Mellon SA/NV, Asset Servicing, Niederlassung Frankfurt am Main, and has its registered office at MesseTurm, Friedrich-Ebert-Anlage 49, 60327 Frankfurt am Main, Germany. It is subject to limited additional regulation by the Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Marie-Curie-Str. 24-28, 60439 Frankfurt, Germany) under registration number 122721. The Bank of New York Mellon SA/NV operates in Poland as The Bank of New York Mellon SA/NV (Joint-stock Company) Branch in Poland with Statistical Number 524311310, whose registered office is at Sucha 2, 50-086 Wroclaw, Poland. The Bank of New York Mellon SA/NV (Joint-stock Company) Branch in Poland is a non-contracting branch. The Bank of New York Mellon SA/NV operates in the Netherlands through its Amsterdam branch at Spaklerweg 4, 1096 BA Amsterdam, the Netherlands. The Bank of New York Mellon SA/ NV, Amsterdam Branch is subject to limited additional supervision by the Dutch Central Bank ("De Nederlandsche Bank" or "DNB") on integrity issues only (registration number 34363596). DNB holds office at Westeinde 1, 1017 ZN Amsterdam, the Netherlands. The Bank of New York Mellon SA/NV operates in Luxembourg through its Luxembourg branch at 2-4 rue Eugene Ruppert, Vertigo Building - Polaris, L- 2453 Luxembourg, Grand Duchy of Luxembourg. The Bank of New York Mellon SA/ NV, Luxembourg Branch (registered the Luxembourg Trade and Companies' Register ("Registre de Commerce et des Sociétés" or "RCS") under number B105087) is subject to limited additional regulation by the Luxembourg supervisory authority ("Commission de Surveillance du Secteur Financier" or "CSSF") at 283, route d'Arlon, L-1150 Luxembourg for conduct of business rules, and in its role as depositary and administration agent for undertakings for collective investments (UCIs). The Bank of New York Mellon SA/NV operates in France through its Paris branch at 7 Rue Scribe, Paris, Paris 75009, France. The Bank of New York Mellon SA/ NV, Paris Branch is subject to limited additional regulation by Secrétariat Général de l'Autorité de Contrôle Prudentiel et Première Direction du Contrôle de Banques (DCB 1), Service 2, 61, Rue Taitbout, 75436 Paris Cedex 09, France (registration number (SIREN) Nr. 538 228 420 RCS Paris - CIB 13733). The Bank of New York Mellon SA/NV operates in Italy through its Milan branch at Via Mike Bongiorno no. 13, Diamantino building, 5th floor, Milan, 20124, Italy. The Bank of New York Mellon SA/NV, Milan Branch is subject to limited additional regulation by Banca d'Italia - Sede di Milano at Divisione Supervisione Banche, Via Cordusio no. 5, 20123 Milano, Italy (registration number 03351). The Bank of New York Mellon SA/ NV operates in Denmark as The Bank of New York Mellon SA/ NV, Copenhagen Branch, filial af The Bank of New York Mellon SA/NV, Belgien, CVR no. 41820063, and has its registered office at Strandvejen 125,1. DK-2900 Hellerup, Denmark. It is subject to limited additional regulation by the Danish Financial Supervisory Authority (Finanstilsynet, Strandgade 29, DK-1401 Copenhagen K, Denmark). The Bank of New York Mellon SA/ NV operates in Spain through its Madrid branch with registered office at Calle José Abascal 45, Planta 4ª, 28003, Madrid, and enrolled on the Reg. Mercantil de Madrid, Tomo 41019, folio 185 (M-727448). The Bank of New York Mellon, Sucursal en España is registered with Banco de España (registration number 1573). The Bank of New York Mellon (International) Limited is registered in England & Wales with Company No. 03236121 with its Registered Office at BNY Centre, 160 Queen Victoria Street, London EC4V 4LA. The Bank of New York Mellon (International) Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Regulatory information in relation to the above BNY entities operating out of Europe can be accessed at the following website: https://www.bny.com/RID. For clients located in Switzerland: The information provided herein does not constitute an offer of financial instrument or an offer to provide financial service in Switzerland pursuant to or within the meaning of the Swiss Financial Services Act ("FinSA") and its implementing ordinance. This is solely an advertisement pursuant to or within the meaning of FinSA and its implementing ordinance. Please be informed that The Bank of New York Mellon and The Bank of New York Mellon SA/NV are entering into the OTC derivative transactions as a counterparty, i.e. acting for its own account or for the account of one of its affiliates. As a result, where you enter into any OTC derivative transactions with us, you will not be considered a "client" (within the meaning of the FinSA) and you will not benefit from the protections otherwise afforded to clients under FinSA. The Bank of New York Mellon, Singapore Branch, is subject to regulation by the Monetary Authority of Singapore. For recipients of this information located in Singapore: This material has not been reviewed by the Monetary Authority of Singapore. The Bank of New York Mellon, Hong Kong Branch (a branch of a banking corporation organized and existing under the laws of the State of New York with limited liability), is subject to regulation by the Hong Kong Monetary Authority and the Securities & Futures Commission of Hong Kong. The Bank of New York Mellon, Seoul Branch, is a licensed foreign bank branch in Korea and regulated by the Financial Services Commission and the Financial Supervisory Service. The Bank of New York Mellon, Seoul Branch, is subject to local regulation (e.g. the Banking Act, the Financial Investment Services and Capital Market Act, and the Foreign Exchange Transactions Act etc.). The Bank of New York Mellon is regulated by the Australian Prudential Regulation Authority and also hold an Australian Financial Services Licence No. 527917 issued by the Australian Securities and Investments Commission to provide financial services to wholesale clients in Australia. The Bank of New York Mellon has various other branches in the Asia-Pacific Region which are subject to regulation by the relevant local regulator in that jurisdiction. The Bank of New York Mellon, Tokyo Branch, is a licensed foreign bank branch in Japan and regulated by the Financial Services Agency of Japan. The Bank of New York Mellon Trust (Japan), Ltd.,is a licensed trust bank in Japan and regulated by the Financial Services Agency of Japan. The Bank of New York Mellon Securities Company Japan Ltd., is a registered type 1 financial instruments business operator in Japan and regulated by the Financial Services Agency of Japan. The Bank of New York Mellon, DIFC Branch, regulated by the Dubai Financial Services Authority (DFSA) and located at DIFC, The Exchange Building 5 North, Level 6, Room 601, P.O. Box 506723, Dubai, UAE, on behalf of The Bank of New York Mellon, which is a wholly-owned subsidiary of The Bank of New York Mellon Corporation. Pershing is the umbrella name for Pershing LLC (member FINRA, SIPC and NYSE), Pershing Advisor Solutions (member FINRA and SIPC), Pershing Limited (UK), Pershing Securities Limited (UK), Pershing Securities International Limited (Ireland), Pershing (Channel Islands) Limited, Pershing Securities Singapore Private Limited, and Pershing India Operational Services Pvt Ltd. Pershing businesses also include Pershing X, Inc. a technology provider.. Pershing LLC is a member of SIPC, which protects securities customers of its members up to $500,000 (including $250,000 for claims for cash). Explanatory brochure available upon request or at sipc.org. SIPC does not protect against loss due to market fluctuation. SIPC protection is not the same as, and should not be confused with, FDIC insurance. Past performance is not a guide to future performance of any instrument, transaction or financial structure and a loss of original capital may occur. Calls and communications with BNY may be recorded, for regulatory and other reasons. Disclosures in relation to certain other BNY group entities can be accessed at the following website: https://www.bnymellon.com/emea/en/disclaimers/eu-disclosures.html. This material is intended for wholesale/professional clients (or the equivalent only), is not intended for use by retail clients and no other person should act upon it. Persons who do not have professional experience in matters relating to investments should not rely on this material. BNY will only provide the relevant investment services to investment professionals. Not all products and services are offered in all countries. If distributed in the UK, this material is a financial promotion. If distributed in the EU, this material is a marketing communication. This material, which may be considered advertising, (but shall not be considered advertising under the laws and regulations of Singapore), is for general information purposes only and is not intended to provide legal, tax, accounting, investment, financial or other professional counsel or advice on any matter. This material does not constitute a recommendation or advice by BNY of any kind. Use of our products and services is subject to various regulations and regulatory oversight. You should discuss this material with appropriate advisors in the context of your circumstances before acting in any manner on this material or agreeing to use any of the referenced products or services and make your own independent assessment (based on such advice) as to whether the referenced products or services are appropriate or suitable for you. This material may not be comprehensive or up to date and there is no undertaking as to the accuracy, timeliness, completeness or fitness for a particular purpose of information given. BNY will not be responsible for updating any information contained within this material and opinions and information contained herein are subject to change without notice. BNY assumes no direct or consequential liability for any errors in or reliance upon this material. This material may not be distributed or used for the purpose of providing any referenced products or services or making any offers or solicitations in any jurisdiction or in any circumstances in which such products, services, offers or solicitations are unlawful or not authorized, or where there would be, by virtue of such distribution, new or additional registration requirements. BNY Wealth conducts business through various operating subsidiaries of The Bank of New York Mellon Corporation. Any references to dollars are to US dollars unless specified otherwise. This material may not be reproduced or disseminated in any form without the prior written permission of BNY. Trademarks, logos and other intellectual property marks belong to their respective owners. The Bank of New York Mellon, member of the Federal Deposit Insurance Corporation (FDIC). Trademarks and logos belong to their respective owners. Please click here for additional information regarding disclaimers and disclosures.