BNY MELLON | PERSHING

Navigating Risk in Today's Uncertain Environment

A GUIDE TO PROTECTING YOUR CLIENTS AND YOUR PRACTICE IN AN EVOLVING REGULATORY LANDSCAPE

Table of Contents

BNY MELLON | PERSHING

Fraud-proofing your business

FRAUD IS SURGING. HERE'S HOW TO PROTECT YOUR CLIENTS AND YOUR BUSINESS

Most advisors think they can see through a fraud attempt, but this is becoming increasingly challenging. Fraudsters continue to find new ways to prey on investors and their advisors. Forget the stereotypical image of hackers working out of basements; many are part of large, well-structured criminal enterprises.

As fraudsters become more sophisticated, they're also more convincing. In some cases, advisors are being tricked by fraudsters posing as clients, using actual details from their lives to sell their deception. Advisors without proper safeguards in place can become targets and subject their business, and their clients, to risk.

Consider fraudsters' success rates in recent years. Five years ago, 10% of reports turned out to be real instances of fraud, according to Rob Hulstedt, Vice President at BNY Mellon's Pershing. Last year that number jumped to 14%. To put this in context, the FTC's Consumer Sentinel Network reported that consumers lost $1.48 billion to fraud complaints in 2018 – a 265% increase over the $406 million they lost in 2017.[1]

In large part, that's because fraud scams have evolved and multiplied. Phishing emails about get-rich-quick schemes and robocalls telling investors they owe hundreds of thousands of dollars to the IRS are just the most obvious, entry-level scams. More sophisticated operations, which in some instances may include technology and linguistic experts, and even attorneys, are highly systematic and focus on how and where they can have the most impact. In other words, fraudsters have become expert impersonators.

It's one thing to fall for a scam when it's your money, but stakes are even higher when you're responsible for someone else's wealth. Having to restore lost funds could put your finances in jeopardy, while the potential reputational damage may jeopardize your client relationships.

While fraudsters are more skilled today, succumbing to them isn't inevitable. By understanding the nature of cyber-fraud in 2020 and how it's likely to change in the coming years, you can develop a plan to keep your clients' assets and your business safe.

Knowing what you don't know

Effective fraud preparedness hinges on an advisor's (and the institution's) attitude towards preparation. At a firm level, it's not enough to design and implement a cybersecurity and fraud training module and then reuse it year after year. Savvy advisors safeguard their clients' assets and their reputations by avoiding complacency and acknowledging what they don't know. The fraud landscape is ever-changing, so ongoing training – with frequently updated modules and an emphasis on best practices – is a must.

For example, at many firms, it's not uncommon for advisors to focus only on the routing and account numbers on incoming wire requests. If those two numbers match what's on record for the client, the request will usually be fulfilled. The problem is that the numbers do match on many fraudulent requests, but deeper digging reveals that the name does not. In essence, what might appear to be a first-party request (usually considered fail-proof) is actually a third-party transaction. In this case, failing to address that detail opens an advisor and the firm to significant risk.

Typically, these steps aren't skipped out of carelessness on the advisor's part. More likely, they're trying to respect the client's time, especially when nothing else appears out of place. For instance, one might not be inclined to verify that a disbursement request is real if it fits with a long-time client's familiar habits and behavioral patterns. Alternately, when an advisor already knows the client has a project on the go, such as a renovation or a real estate purchase in the works that requires a transfer of funds, this may not trigger the need for additional diligence.

But the idea that fraudulent communications will always be easily identified – either because they're riddled with grammar and spelling mistakes or contain inadequate or inaccurate identifying information – is wrong.

Fraudsters use proofreaders and have perfected the art of email hacking. As a result, they often have access to a wealth of personal information – including passwords, account numbers and knowledge of significant life events and recent transactions. And even if you know your client's voice and mannerisms well, your colleagues – who might be on the receiving end of a fraudulent request delivered over the phone – probably don't.

The gold standard of fraud detection

Apart from ensuring anti-virus/malware software and firewalls are installed and up to date, preventing fraud doesn't require special tools or technology. What it does require is a consistent focus on the potential for security breaches and how to identify them accurately. In other words, a proactive mindset and a handful of simple behaviors will protect your clients and your business from attack.

Common sense and a simple phone call are the gold standards for fraud detection. All wire transfer requests an advisor receives, even if they look legitimate, merit a follow-up phone call on the investor's phone number of record.

Is the request consistent with past activity? Has the client already told you he was thinking about renovating and now he's emailing with a contractor's invoice and a disbursement request? When in doubt, make the phone call. Four out of five fraud attempts are stopped this way, says Hulstedt.

Additional measures like verbal passwords are helpful, too. Sometimes you won't reach the client right away, and that's okay. A good best practice here is to wait until you can. Most legitimate requests won't have the same urgency as a fraudulent one, and if the client does express irritation at having to wait, explaining that it's for security reasons will mitigate it. The same goes for last-minute requests to call the client at a different number – a big red flag. Without exception, always call the client on the established phone number of record.

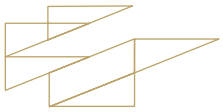
Of course, understanding the importance of the follow-up phone call, in theory, doesn't guarantee you'll remember to use it in practice. Both investors and advisors need regular opportunities to reinforce their knowledge and their habits.

For advisors, this opportunity usually takes the form of internal training and frequent information sharing with peers and partners like Pershing. And investors are best served when their advisors share this information with them, as well.

The fraud landscape in 2020

An obvious place to start any security fraud training is with an updated list of current threats, their frequency, and their impacts. Today, that list is long and growing. It includes:

- Email compromise
- Malware
- Ransomware
- IRS impersonation scams
- Robocalls/unsolicited phone calls
- Sweepstake/lottery scams
- Elder financial abuse
- Text scams, targeting millennials on their smartphones



- Grandparent scams, where fraudsters pose as grandchildren
- Romance/companionship scams, where fraudsters act as romantic interests
- Identity theft
- CEO scams, where fraudsters pose as a CEO asking for high-value gift cards for employees
- Real estate scams

Real estate fraud is by far the fastest-growing threat today. Between 2016 and 2018, rates increased by 1,100%, says Hulstedt. And it's no wonder why. Fraudsters have learned they have more success when they time their transactions to coincide with real events happening in investors' lives – one typically surrounded by intense pressure and stress, like a real estate purchase.

Hulstedt says the exchange typically goes something like this: "Fraudsters pose as the investor and communicate with the advisor, either requesting a wire transfer directly or asking that it be sent to the title company. Then, 20 minutes before the house closing, they'll change the account number."

Nina Weiss, Chief Compliance Officer at Pershing, says ransomware cases, in which fraudsters hold an advisory firm's computing system hostage for money, are less prevalent today. But email hacking is on the rise, and investors are especially vulnerable when they reuse passwords.

With enough information, fraudsters may be able to copy signatures or intercept email threads. "Fraudsters will use bots to comb through literally every single document you have stored on your computer," says Hulstedt. "It's very, very easy." Hulstedt describes a case at Pershing he learned about recently: after three weeks of emails between investor and advisor, a fraudster took over the investor's email account and asked the advisor for a wire transfer of $400,000 (fortunately, the advisor called the investor to confirm before initiating the transaction).

Note that check fraud – a very slow process – is essentially off the radar. Most scams today are third-party requests for wire and electronic bank-to-bank (ACH) transfers, which are practically immediate.

Third-party fraud is also known as "true identity fraud," because it involves a fraudster impersonating an investor to open new accounts or take over existing ones without the investor's knowledge. The real end game for many fraudsters is to take those funds out of the United States, to countries that don't have extradition treaties, putting them out of reach from authorities, explains Hulstedt.

Remember what's at stake

Many advisors are busy and recognize their clients are busy too, which can lead some advisors to take shortcuts that they think will make the client happy. It's easy to argue, for example, that when a wire request appears to be consistent with what's happening in the investor's life, the risk of fraud is so small there's no need to follow up. Or that a client is very busy and doesn't like being interrupted, regardless of the reason.

The solution in both cases is to remember that fraudsters are smart and getting smarter. As an advisor, you can't afford to assume it can't or won't happen to you. And when it does, following up with a phone call is still the best safeguard available.

Yes, some clients might be irritated by this extra step, but setting the expectation – that there will always be a follow-up phone call, and it's for their protection – at the outset helps. "And in the end, it really comes down to which phone call you'd rather make," notes Weiss. "The one you're making to keep your clients' assets safe, or the one where you tell them they just lost $400,000."

Fraud training best practices

Even more important than the specific content of fraud training, whether targeted at advisors or investors, is the "tone from the top." That is, advisors who are true stewards of their clients' savings have leaders who do all they can to protect themselves from being victimized – because when fraud does occur, everyone is a victim.

With a culture built around proactive preparedness, firms are more likely to produce high-quality fraud training and information-sharing opportunities that do three things:

1. Give advisors and investors the information they need to avoid becoming victims of fraud
2. Emphasize the need and teach your advisors how to supplement this knowledge on their own on an ongoing basis
3. Coach your advisors on the specific mindset and habitual behaviors that will protect them from fraud

What's more, these learning opportunities will likely happen on an ongoing basis, with a cadence that matches the rapid pace of change in the fraud landscape.

What's in the box

As part of this package, Pershing includes timely data on fraud (e.g., number of successful attempts last year, dollar amounts, etc.) as well as specific guidance on cultivating good habits, both mental and behavioral. For example:

1. When fielding requests from elderly clients who might have diminished cognitive function, speak with a trusted contact person.
2. Elderly or not, always follow up on a client's emailed request for a transfer with a phone call to the client's number of record, regardless of the size of the transaction.
3. On the phone, ask for specifics: "Did you send me this request, for this amount, to this account?" Asking an additional authentication question is even better.
4. After you've called, sign an attestation to that effect.
5. If instructions change or there was a hand-off to a colleague somewhere in the process, document that the call was made.
6. Actively engage regulators and law enforcement in identifying and addressing fraud risks.

In addition, Pershing points our clients to valuable external resources like the OCIE's Cybersecurity and Resiliency Observations. This annual report offers additional suggestions on how advisors can stay informed between formal training – signing up for alerts from CISA, for example, checking the SEC's cybersecurity page, and participating in information sharing groups through industry organizations.

It's important to educate your clients as well. The goal is to develop an investment policy statement that identifies each client's short-, medium- and long-term goals, and sets the expectation that any request that deviates from the plan will trigger a follow-up phone call from the advisor.

Just like for advisors, frequent updates – via newsletter, blog post or both – are essential, as is a regular cadence of client meetings focused on best practices for detecting fraud. Advisors who take these steps help to preserve their reputations along with their clients' assets. And their businesses are positioned to grow as a result.

Choose the right course of action

When a fraudulent transaction does get through, the consequences can be severe. Hulstedt says the fraudster will immediately take the funds from the contra firm and move them to a different institution, and then it's up to the advisor to make the investor whole. "Error and omissions insurance doesn't always help," he cautions. "They won't cover you if you can't prove you took all the necessary precautions."

He's even heard of advisors having to write checks from their personal accounts. While an instance of fraud could be painful for a larger firm, depending on the dollar amount, it could force a smaller one to close its doors.

On top of the immediate financial risk, restoring an investor's assets after a fraud is a complex, lengthy process. Not only does the advisor have to replace all of the investor's trades from the transaction date, but money taken as taxes has to be recovered from the federal and state governments too. And when that process is complete, there's still the issue of reputational damage. Larger advisory firms will usually cut ties with an advisor implicated in fraud, not wanting to risk losing clients over a perceived lack of integrity. And solo advisors are particularly vulnerable. Once their names are sullied by an incident, keeping existing clients and acquiring new ones becomes a herculean feat.

Learning how to protect your clients and your business from security fraud is much easier. But even more importantly, it will reinforce your role as a trusted advocate and enhance your relationships with clients.

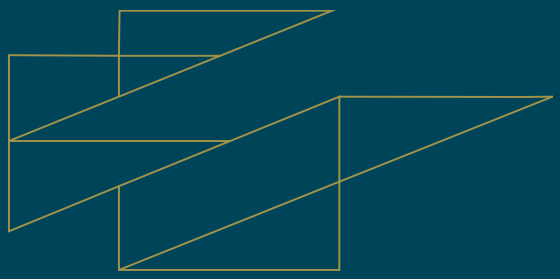
As a custodian and a partner with stringent risk controls, Pershing is well positioned to keep you abreast of the latest fraud trends and help you share that information with your team. We hold regulatory and compliance webinars to share this information, and we're also able to keep you up to date on the latest news from regulators about the threats they see on the horizon.

At BNY Mellon's Pershing, we favor overcommunication, both internally and externally. There's a monthly compliance forum for every advisory firm we partner with – 503 in total – which is open to all their employees. We also send a weekly newsletter to all our clients, which includes the most current information we have on policy changes, recent developments in the industry as a whole and new scams on the horizon, as well as an annual presentation specifically around fraud.

We encourage each of our clients to call us on an ad-hoc basis with questions – we're always available to discuss best practices in this space. By working together, we can help you stay a few steps ahead of fraud, so you can focus on serving your clients.

[1] "Consumer Sentinel Network: Data Book 2018," Federal Trade Commission (February 2019) (accessed on April 29, 2020).

BNY MELLON | PERSHING



Cybersecurity in an increasingly complex world

SAFEGUARD YOUR BUSINESS AND YOUR CLIENTS FROM CYBERCRIME

Thieves have been trying to break into banks to steal money long before the Internet. At the time, thick concrete walls and heavy metal doors were among the strongest defenses against crime. Today, your clients' assets can be placed at risk because theft can take place practically in thin air as cybercriminals use technological means to steal information or assets. Although technology is making it easier to rebalance portfolios, draw up financial plans and communicate with clients, it's also creating a new set of challenges to defend against in your practice.

The perpetrators of cybercrime are not only keeping pace with advancements in technology, but they are also often on the leading edge – and the stakes are high if you don't take appropriate steps to protect your systems. When you're responsible for someone else's wealth, the risks extend far beyond the possibility of actual money being stolen: the reputational damage it may cause you and your firm can be even more devastating.

Cybersecurity breaches come in several forms, be it a virus infection through email, the introduction of fake, malicious websites (malware), the implementation of phishing schemes or other applications that might expose framework or system vulnerabilities. The attack may attempt to exploit internal and third-party provider vulnerabilities for financial gain or cause business disruption.

There is a growing imperative for advisors to embrace change and adopt new technologies, yet RIAs may not have a large technology infrastructure supporting them. The challenge will be for RIAs to ensure that their practices and their clients don't become the targets of cyberattacks.

With the constant threat of cyberattacks, it's not surprising that financial services firms are expected to continue ramping up cybersecurity spending, which could reach $43 billion globally by 2023.[1] For larger firms, added costs are painful but not prohibitive; the same cannot be said for smaller firms and RIAs.

Yet, as evidenced by recent breaches, the cost of inaction can be even higher. In recent years, highly publicized cybersecurity breaches have made the news. Target Corp. endured one and so did Equifax Inc. – just to name two high-profile cases. In 2017 alone, the average cost of a data breach was $3.62 million.[2] Financial services firms understand it is a priority to uphold effective cybersecurity policies, and that consequences will ensue if they don't.

For the past eight years, the Office of Compliance Inspections and Examinations (OCIE) for the U.S. Securities and Exchange Commission (SEC) has placed cybersecurity on its examination priority list. Recently, the OCIE released its cybersecurity and resiliency observations, which provide practical guidelines of what to look for and what the OCIE has been observing in the advisory industry. For instance, the OCIE noted that effective cybersecurity programs greatly benefit from a commitment by a firm's senior leadership to understand cybersecurity risks and prioritize the communication of these risks across the organization so they can mitigate them. Robust risk assessments, strict access controls and comprehensive testing of cybersecurity programs and systems are three of the best practices to follow.

Recognize your vulnerabilities

Using technology to fight technology offers a layer of protection, but technology alone isn't the answer. Advisors also need to be aware of the threats and vulnerabilities they're up against so they can know how to guard against them in order to protect themselves, their firms and their clients.

Ransomware

One major theme pertains to ransomware, where criminals threaten to publish the victim's data or prevent access to this data unless the victim relents to a specified financial transaction (known as a "ransom"). These actors typically demand wire transfers or other electronic means to extort money from the victim, as digital methods are harder to trace.

For issues like ransomware, it's critical to have reliable offsite backups and a business continuity plan that incorporates the use of those offsite backups. If an actor encrypts all your data or denies access to your servers, then you can use your backup to safely restore your systems. Although disruptive, it means you can resume business operations through another provider until your ransomware issue is resolved.

Denial of service

An important but often overlooked topic is the denial of service. That's when actors will initiate disruptive actions like overloading your network traffic or send innumerable requests in an attempt to deny people from getting work done. For example, Robinhood Financial experienced a massive service outage during a steep market decline, but nobody on Robinhood's system could execute a trade. So, the firm faced legal action by clients who lost money when they couldn't make trades as markets plummeted.

Robinhood identified the situation as a system malfunction, but it's also possible that someone flooded its system's front-end interface or inundated its website with traffic, denying access to anyone else. Larger firms have intricate filtering services and implement denial of service controls to address such problems.

Stolen credentials

Whenever you send client information, failing to conduct the proper checks and follow established security procedures can leave this sensitive data vulnerable. One of the most common cybercrimes involves people who pose as clients by stealing their credentials. The criminals try to lure you into communicating with them instead of the actual client to trick you into sending them a client's personal information.

In addition to limiting the exchange of client data, one of the best ways to protect yourself from criminals who pose as clients is to be trained on the latest techniques and approaches that criminals use so you can recognize scams and avoid falling victim to them.

Good cybersecurity is more than technology

Combatting cybersecurity issues requires significant training and awareness, both internally for firms and for clients. It extends beyond technology and involves vigorous, up-to-date education. The SEC has recommended that firms address governance and risk management, which involves having senior-level engagement in cybersecurity and resiliency strategy.

An important element of a cyber resiliency program is developing and conducting risk assessments. List your actual and potential cyber risks, where these risks may exist and what issues they may cause. Aside from technological aspects like firewalls and access controls, a good risk assessment involves understanding risk mitigation processes. For example, do employees know their role in cybersecurity? If an employee is a point of escalation, he or she should know exactly what the next steps would be if an escalation occurs.

Another valuable non-technology action is regular testing and monitoring of the entire cybersecurity program to ensure all measures remain relevant and effective. A firm's cybersecurity program includes comprehensive policies and procedures that must be

clearly documented. To validate the effectiveness of these policies and procedures, the firm must adopt a robust testing, monitoring and evaluation regimen – on both a scheduled and unscheduled basis – using available cyber threat intelligence to help set parameters. If any audited policies or procedures fail to fulfill their cybersecurity functions, the firm must promptly address those systemic gaps or deficiencies.

Securing the home office

With many people working from home on an ad-hoc basis or as part of their regular work schedules, a major challenge is taking extra care in managing information. At the workplace, you're inside a secure enclave with the ability to protect client information. At home, if you print sensitive files, assemble folders for clients or have paper containing sensitive client information, you must follow established protocols to protect the data.

Practice vigilance with passwords

We encourage using one-time passwords (part of two-factor authentication), in which a person logging into an account will receive a text message with an authenticating number to use. That extra layer of security helps reduce account takeovers as cybercriminals can't easily take over these accounts because access relies on more than a single password.

Recently there has been a significant attitude shift toward one-time passwords. Most people still consider the practice to be bothersome, but they recognize its importance for good cybersecurity and accept it.

Security tips for working from home

1. As a general rule, minimize printing. When you must print sensitive paperwork, dispose of it by shredding or locking it up to prevent misuse.
2. Think of your home as an extension of your workplace and adhere to the same risk protocol. If possible, work in a space that can be properly secured.
3. Examine how you're accessing your work systems. If using a personal computer, it may not have the same level of security controls as your machine at work, so install updated anti-virus software and other base controls.

Tips for firms with employees working from home

1. Consider instigating system controls to prevent remote printing and utilize encryption technology to protect the exchange of data.
2. To prevent unwanted access, promptly revoke all credentials of employees who have left the company and purge inactive accounts to remove them from your system.

Potential consequences of cybercrime

On top of ransomware issues and phishing expeditions, vulnerabilities exist when people use third-party vendors. If a vendor encounters a cybercrime, advisors need to assess their vulnerability. What customer account information is out there and what other sensitive information is shared with that vendor?

Advisors who don't take adequate cybersecurity measures could lose a lot of money – and their businesses. When a trade is missed or a client claims something wasn't done properly, the client will need to be made whole again. So there's real money at stake for advisors and their firms. If you encounter a ransomware situation, not only would you be unable to conduct business, but you could also lose significant money in fines and credit monitoring, given that client data might be at risk of being lost and misappropriated.

Although there are financial consequences if you fail to sufficiently protect your clients, there may also be a reputational consequence that could severely harm you and your firm's brand and compromise the trust you've established with clients.

Regulatory consequences of cybercrime might result in anything from a fine to extra disclosures, but these are clear and finite penalties. A reputational loss, however, is harder to quantify and difficult to overcome. Clients are more educated than ever and will ask questions about system safety measures for ensuring the confidentiality of personal data. Increasingly, clients understand the importance of cybersecurity and the value of keeping their information secure. If you don't deliver on your security commitments, your reputation (and your firm's) may be damaged, and in today's connected world of mass media and social media, the damage may be substantial.

Be educated and prepared

How do you maintain good cybersecurity practices? It's an ongoing process. Advisors can take proactive measures to help protect clients. Being educated is crucial and advisors need a robust cybersecurity program to reference and follow. The OCIE has created a basic framework regarding the need for implementing strong technology, policies and procedures. Also, consider your resiliency program because you will likely have to deal with cybersecurity threats at some point.

Cybercriminals are getting smarter and more deceptive, with access to better technology and tools. The more you and your firm educate yourselves, the more you can do. Keep apprised of the SEC's releases and what they're saying. The SEC recommends sharing information through its financial services information sharing and analysis center.

Compare the National Institute of Standards and Technology's (NIST) cybersecurity framework to your own, as the NIST framework is worth emulating. Another useful organization to reference is the American Institute of CPAs (AICPA). The AICPA's System and Organization Controls reporting framework enables organizations to communicate information about their cybersecurity risk management program to help satisfy stakeholder cybersecurity information needs.

It's also strongly advised to designate at least one person at your firm to stay current with cybersecurity news and trends. Sharing information lets you learn about other firms' experiences and exposes you to best practices that you can adapt. There are no one-size-fits-all cybersecurity solutions, so be aware of what's out there and customize relevant practices for your firm.

Good education, awareness and training also allow you to take immediate action if a cyber breach occurs. If you're scrambling when you encounter some type of failure, that's a problem. Have a robust plan and test it often. You should have a clear plan of what you need to do, what systems are affected, which people to engage and what notifications to issue. Gather as much information as you can to make the best decisions possible.

Your set protocol for dealing with cybersecurity issues may include notifying your vendors, partners and internal team. Will there be a shutdown? If so, what's your contingency plan

and how does that roll out? If you work with a partner (such as BNY Mellon's Pershing) and advise that you've experienced a threat or successful cybersecurity issue, what can be done if you're offline? What can your partner do, what do you need to know and whom should you contact? Those are questions you must answer to help inform a robust resiliency program that can keep your firm and clients protected.

Assessment checklists are crucial

It's good practice to house your cybersecurity policies and procedures in a comprehensive catalog of risk assessment. Check them regularly and make updates, as required, and make your team aware of these policies and procedures. It's only valuable to have them in place if everyone knows where they are and what they mean.

Going through an assessment checklist – and amending it when needed – should be an annual exercise or performed whenever you experience a notable change (e.g., if you absorb or merge with another business or switch service providers).

> "The Federal Financial Institutions Examination Council (FFIEC) offers a useful security self-assessment. It's a cybersecurity checklist that's available for free on the FFIEC site. We recommend this self-assessment to our broker-dealer clients."
>
> *-Jeffrey Davis*
> *Director, Sr. Group Manager, Information Security, BNY Mellon's Pershing*

How we can help

Pershing is committed to helping clients (and their clients) with cybersecurity. For instance, our leading-edge "rules engine" allows broker-dealers to set parameters. If a transaction is beyond a certain dollar threshold or if a 401(k) account starts making uncharacteristic, high-volume transactions that resemble day trading, the rules engine will flag that and require additional authorization. That's one way advisors and broker-dealers can keep abreast of transactions.

> "The customizable rules engine is part of our system. Our clients can configure it or ask their relationship manager to help with configuration, and they can decide which rules they want to implement and which ones they don't."
>
> *-Nina Weiss*
> *Chief Compliance Officer, BNY Mellon's Pershing*

The rules engine includes a base set of recommended rules – numbering into the thousands – with thousands more from which advisors may select. In addition, BNY Mellon's Pershing Advisor Services takes many actions on the back end to ensure our systems are secure by searching for vulnerabilities through penetration testing and vulnerability scanning. A third party performs assessments on our systems and issues a cyber trust certificate that attests to system security, while our ISO 27001 certification is updated every three years.

Other ways we support you

Pershing can help develop and support your firm's resiliency programs, so you have a viable plan that maps out the steps you need to take and the people (such as vendors) you need to contact, as well as determining who needs support in the event of an outage.

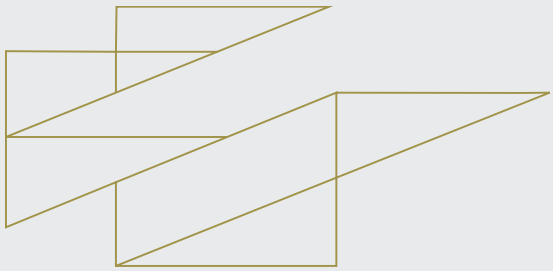
For advisors who want to help clients keep their systems secure, we can advise if they need to run the latest anti-virus software, if they should be utilizing factor authentication or one-time passwords, and why they shouldn't use common passwords for different systems. After all, if one of those accounts gets compromised, the cybercriminal may try the same credential against other related accounts.

As a custodian and a partner/vendor with its own stringent risk controls, BNY Mellon's Pershing is well positioned to add a nuanced perspective in this area. As the area of cybersecurity is constantly evolving, we hold regulatory and compliance webinars as an avenue to relay timely information. On our annual security and fraud webcast, we share what we're hearing from regulators, what new cybersecurity rules and regulations might be on the horizon, and common best practices. Whenever we learn anything new, we disclose that in releases to our advisory clients. It's all about providing the best possible technology and support to bolster our clients' cybersecurity.

[1] Rouse, Tim. "Cybersecurity poses strain between plan sponsors, record keepers," InvestmentNews.com www.investmentnews.com/cybersecurity-poses-strain-between-plan-sponsors-record-keepers-78751 (accessed on April 16, 2020).

[2] van Kessel, Paul. "Is cybersecurity about more than protection?" ey.com (accessed on April 16, 2020).

BNY MELLON | PERSHING



Adapting to a shifting regulatory environment

UNDERSTAND THE LANDSCAPE AND BE POSITIONED FOR SUCCESS

The financial services industry has always been highly regulated – and rightfully so, given what's at stake. In recent years, regulatory reform has intensified as more complex challenges arise and more emphasis is placed on protecting end clients as well as those who serve them.

Although the industry may consider today's increased regulatory and compliance oversight to be a necessary but cumbersome aspect of conducting business, heightened regulatory measures are designed to benefit those who are willing to embrace them as a means of differentiating themselves from the competition. After all, since evolving regulations are primarily intended to safeguard investors and mitigate risk, getting on board with these regulatory initiatives could be a proof point that advisors and their firms offer value to clients and have their best interests in mind.

At BNY Mellon's Pershing, we take a collaborative, consultative approach to helping you manage and grow your business. If you're interested in regulatory issues like data protection, cybersecurity and fraud, we have explored each of them in individual whitepapers.

Although the aforementioned issues tend to garner significant attention and make headlines in mainstream and financial media alike, other important topics are also part of the trend toward improved regulation and protection. They include, but are not limited to, the following:

- Regulation Best Interest (Reg BI)
- Form CRS, the new client relationship summary
- Financial abuse of seniors/elders

These three topics are highly relevant to Security and Exchange Commission (SEC) registered investment advisers (RIAs) who work with retail investors, and broker-dealers registered with the Financial Industry Regulatory Authority (FINRA).

Reg BI: A Higher Level of Client Care

The SEC states that Reg BI is a standard of conduct for broker-dealers whenever they make a securities recommendation to retail investor clients. Reg BI goes beyond traditional suitability obligations. It aligns conduct standards with retail clients' reasonable expectations by requiring broker-dealers to act in the best interest of these clients, rather than their own. If a conflict of interest is not reasonably addressed by a full disclosure of material facts, the broker-dealer must take actions that can mitigate or eliminate this conflict.

One of the practical applications of Reg BI involves share classes of mutual funds. For instance, when considering Class A, B or C shares, it's clear that each class has a different fee structure and their suitability depends on a retail investor's particular financial and time-horizon circumstances. Under Reg BI, the broker-dealer must invest the retail client's assets in the share class that's most beneficial for this specific client, regardless of the impact on the broker-dealer's compensation.

Such a requirement involves "regular monitoring of accounts and portfolios," says Michelle Logue, Pershing's Chief Compliance Officer. "You can have the lowest-cost share class today and next week that could change, which means ongoing administration and research are essential. Since the regulators may consider it a suitability issue or a potential risk-execution issue, it's something that broker-dealers need to focus on to ensure the client's best interests are met."

While the goal is always to eliminate conflicts of interest, it is not always possible. In such cases, the risk either needs to be mitigated or fully disclosed. Given that it's extremely difficult to anticipate whether or not the regulators will be satisfied with particular mitigation or disclosure efforts, the most practical course of action is to be as transparent as possible and always do what's best for the client.

Another significant challenge pertaining to Reg BI is that certain states are introducing different rules. For instance, Massachusetts, through its Fiduciary Rule, has recently enacted a requirement for sales content (to be enforced starting September 1, 2020) that is an amendment of Reg BI. This means that traditional broker-dealers who produce sales content directed at retail clients in different states will need to be mindful of the variances regarding standard of care. In the case of Massachusetts, the standards are more rigorous than Reg BI and stipulate that disclosure alone is not sufficient. Every reasonable effort must be made to avoid conflict of interest; if unavoidable, then the conflict must be mitigated or eliminated. Other states may eventually proffer their own interpretations of Reg BI, potentially leading to a fragmented regulatory environment.

Form CRS: Enabling apples-to-apples comparisons

The SEC requires registered investment advisers, registered broker-dealers and dually registered firms to provide an easy-to-understand client relationship summary (Form CRS) to retail investors. For single registrants, the summary cannot exceed two pages, while the limit is four pages for dual registrants.

The intent of this concise, plain-language summary is to inform retail investors about the various types of client relationships and services that the firm offers, as well as the costs, standard of conduct and potential conflicts of interest related to these relationships and services. Also included under Form CRS is a declaration of whether the firm and its financial professionals have any reportable legal or disciplinary history, as well as explicit direction to investor education resources related to investment advisers, broker-dealers and financial professionals. Retail clients will receive Form CRS at the start of their relationship with a given firm, as well as updated information should there be any relevant material changes. Form CRS allows investors (i.e., potential clients) to easily compare relationships and services of different firms, helping them decide with which firm they wish to conduct business.

If you require assistance regarding Form CRS, Pershing has created two documents to help you:

- Getting Started with Form CRS provides a checklist and considerations for content, processes, delivery and recordkeeping.
- Client Guide for SEC Client Relationship Summary (Form CRS) offers practical guidance, section by section, on how to produce a robust, comprehensive Form CRS.

Addressing Elder Abuse in the Industry

Another major regulatory focus in recent years has been on the protection of seniors and vulnerable adults against fraud or otherwise being financially mistreated by industry professionals.

> "Everyone is aware of this topic and it has broad relevance for the industry and its regulatory bodies. We spend considerable time educating advisors on current schemes and frauds. It's heartbreaking to see trusting, vulnerable seniors being taken advantage of in any manner."
>
> *-Joan Schwartz*
> *Chief Legal Officer, BNY Mellon's Pershing*

A recent FINRA proposal seeks to prevent registered representatives (non RIAs) from acting as beneficiaries on certain accounts belonging to seniors. Some people in the advisory space exert undue influence on elderly clients and become so close with them that they eventually take on positions – like an executor, trustee or administrator of an estate – and then the client chooses to gift assets to them upon their passing, which becomes an obvious conflict of interest. Unfortunately, as the U.S. population continues to age, the industry should expect more of these issues to surface.

Elder abuse remains a major concern as it ties into the trust of the investing public. The industry bears much responsibility for providing the services required to save for education (e.g., helping to send children/grandchildren to college), retirement and all of life's needs. It would be prudent for advisors and their organizations to take a firm, proactive approach to avoiding or mitigating risks associated with seniors and their financial wellbeing.

RegTech Can Help Facilitate Compliance

In order for advisors to securely monitor and manage regulatory processes, regulatory technology tools (RegTech) may be a cost-effective solution. For instance, depending on the situation, Form CRS either has to be delivered at the time the recommendation is made or the time when the advisory agreement is signed. The financial industry as a whole must determine what is the optimal mechanism for delivery and come to a mutual agreement. From a RegTech perspective, electronic delivery of Form CRS would clearly help with the timing while also satisfying compliance requirements.

With regard to broker-dealers, Form CRS is complicated because not only must they deliver at the time of the recommendation, but if the retail investor never opens an account, the firm still has to document and retain the information for a period of time that the investor had been provided with a recommendation that constitutes part of the Form CRS requirement.

When implementing technology around the delivery of Form CRS, the key steps would include entering a form into the system, inputting the proper information and then delivering it. The advisor doesn't have to provide the documentation until the advisory agreement is signed. Given this timing, many advisors have elected to make Form CRS the first two pages of their advisory agreement. This way, they can demonstrate timely delivery and client signoffs, which helps simplify the compliance process.

RegTech may also be valuable from a regulatory and compliance perspective in terms of protecting sensitive information (via secure data storage and document encryption), employing system risk controls to help thwart hackers and maximizing the efficacy of digital signature technology.

Diverse Impacts of Regulatory Reform

The rollout of new regulations and compliance standards has illustrated how various industry members are affected differently. For instance, broker-dealers are now comprehending the finer points of the entire process. From their perspective, it's a different way of conducting business and involves a shift in mindset. If a client has a brokerage account, then their firm provided them with a Form CRS when they opened that account. But what if the client later decides they want to move to an RIA? Once the move has been completed, the client's account is tagged as "RIA" with an affiliated RIA of their broker-dealer. The move could result in the client having to receive another Form CRS. This duplication is just one of the many variables that everyone in the industry needs to consider and work out in an efficient, logical manner.

The financial industry is counting on regulators like the SEC and FINRA to provide strong guidance in terms of defining clear regulatory roles and responsibilities. This guidance would help firms that are presently not fully advisory to make smoother transitions and better understand what's expected of them as they attempt to refashion their business.

If an advisor is standalone and SEC registered, then Reg BI and Form CRS should have minimal impact. Although Form CRS is required as Part Three of the Form ADV and advisors must follow a standard template, for such firms these actions represent little more than a perfunctory obligation.

However, for firms like broker-dealers that are affiliated with advisors, it's a bigger task. Advisors with a broker-dealer connection likely don't have a Form ADV responsibility, so satisfying all of the Reg BI disclosure requirements is a significant undertaking. Yet, since Form CRS is limited to two pages and is formatted in a set template, meeting these new compliance standards becomes less onerous.

For the typical RIA, Reg BI likely won't be impactful because this regulation is largely focused on enhancing the duty and care standards in the broker-dealer segment. In terms of Form CRS, given that it's an add-on to their existing Form ADV, the primary concern for RIAs is to execute in a timely fashion. RIAs are more intent on implementing and maintaining strong controls on their technology to protect client information from privacy or cybersecurity breaches. One of their primary objectives is to gain the trust of the investing public and encourage them to pursue the benefits of fee-based advice.

It's important for RIAs to find an effective way to distinguish themselves as being entrenched in the true advice and planning business, where they can help clients with all their financial needs while committing to a higher (fiduciary) standard of care. RIAs holistically address a client's life, from investment strategies and tax planning to debt/liability management and more. It's important for RIAs to continue discussing the value they create for clients within the fee-for-service business model.

We're Here to Support You

At Pershing, we are resolutely focused on staying abreast of all regulatory matters and educating our clients. On behalf of both the regulators and the advisors on our platform, we work tirelessly to find and implement solutions that help them achieve compliance. We also hire experts to try and "poke holes" in our industry certifications. The overarching aim is to give advisors some comfort and peace of mind.

> "Clients value our focus on key regulatory requirements and the strength and stability we provide as custodians. Since we service different business models the way they want to be serviced and connect our technology with other technology platforms, advisors can receive the comprehensive, tailored offering they need."
>
> *-Joan Schwartz*
> *Chief Legal Officer, BNY Mellon's Pershing*

Custodians fulfill an important role in the industry by managing a significant portion of the regulatory burden – something most firms are not able to take on. Clearing firms like Pershing provide the investing public with many opportunities. The independent (i.e., third party) clearing model, which is distinct from the self-clearing approach, creates much greater choice, especially for smaller investors.

After all, not everybody has an account big enough to be serviced by the larger firms. Whether they're millennials, seniors or anyone in between, many people lack the capacity to earn and save enough money. Whatever they are earning, the industry wants to help them save as much as possible. Regardless of a given firm's business model, one of the industry's unifying aspects is that everyone genuinely wants to provide meaningful service and good value to the investing public, to help them reach their financial objectives. Accordingly, the entire industry is motivated to collaborate and exercise regulatory vigilance.

"We're at a pivotal time where the competitive walls must come down at times, especially from a regulatory perspective, so we can all be on the same page" Pershing's Michelle Logue says. "We spend considerable time in various industry groups discussing regulatory issues and figuring out what's best for the client and the industry. We all take great pride in this common and worthy goal."

Regulatory Resources

As part of our commitment to educating clients on important regulatory issues like Reg BI and Form CRS, Pershing offers downloadable presentation decks as well as webinar sessions where we can address your questions. For your reference and convenience, we also make available recent FAQs issued by the SEC on relevant regulatory matters.

BNY MELLON | PERSHING

Navigating the new regulatory paradigm for privacy

DATA MANAGEMENT FOR TODAY'S (AND TOMORROW'S) ADVISOR

Data protection, privacy and disclosure are sometimes nothing more than business buzzwords. But more often they represent a deep, enduring trend as technological advancements intersect with an increased vigilance regarding the use and ownership of personal information. Recent high-profile data breaches involving Facebook, Cambridge Analytica and Google (to name just a few) are shining an even brighter spotlight on issues like transparency and data protection.

No industry is immune from this changing landscape – certainly not financial services, with its rigorous regulatory oversight, dependency on data collection and inherent reliance on third-party data providers, digital record-keeping and vendor management.

Major regulatory reforms like the European Union's General Data Protection Regulations (GDPR), introduced in May 2018, or the California Consumer Privacy Act (CCPA) may not seem to impact advisors outside of Europe and California, but such advisors would be wise to become familiar with them. Not only are GDPR and CCPA harbingers of sweeping data-related reform to come, but they may also affect advisors who are based beyond the current regulatory jurisdictions.

Defining personal information

It's well documented that the primary objective of GDPR is to protect the privacy rights of individuals by standardizing and restricting how organizations collect and process personal

data. The onus falls squarely on the shoulders of such organizations (or "data collectors," as characterized in GDPR terms) to own the data management lifecycle. The CCPA provides consumers with certain rights regarding how organizations collect, sell or otherwise share their personal information.

What is involved in meeting all of these enhanced data management responsibilities? The task includes:

The initial data collection

Disclosures to the consumers

Storing and securing of information

Processing and transferring information

Data anonymization or aggregation

Disposal and deletion of unneeded information

Over the years, authorities have cast a wider net regarding what is considered personal information, and individuals now have a greater ability to access and control what personal information businesses are holding. For instance, Facebook now allows users to download all of their data, see which advertisers have uploaded their information to a contact list, and control how the service manages any location data it has collected from their mobile devices. In other words, consumers are more empowered than ever before and this trend is poised to continue.

For organizations that breach any of their data management requirements, the levying of potentially severe fines and penalties has dramatically increased as new privacy laws take effect. Regulators hold more influence now and are doing more as well, so American advisors should care about client privacy and data management. When the European Union rolled out GDPR, many data collectors in America examined their businesses and concluded that they don't have any direct exposure because they are not targeting services to residents in the European Economic Area (EEA). In fact, many American businesses may not have complied with GDPR, or even made an attempt, because they weren't prospecting and working with European residents.

But laws like GDPR and CCPA are "extra-territorial." They are not concerned with the location of the organization itself as a business entity that's processing sensitive personal information. They are concerned, however, with the residency of the individuals whose information is in question. So it's a matter of California residents' information being processed anywhere in the world, or EEA residents' information in Europe being processed anywhere in the world. If one of your clients moves to Europe or California, for example, then GDPR or the CCPA will apply and you'll need to comply with the new privacy laws in those regions.

Evolution of regulatory stringency

GDPR has become the de facto baseline for data management compliance, but it's not as simple as saying that complying with GDPR means you're complying with similar laws around the world. It simply means if you comply with GDPR, you've got the highest possible baseline. We have specific laws in America, such as the Gramm-Leach-Bliley Act and Regulation S-P, that require financial institutions to divulge their practices regarding personal information sharing and protection.

Nonetheless, the Gramm-Leach-Bliley Act does not address issues pertaining to modern technology. Under the old framework, there was "nonpublic personal information" (NPPI), such as an individual's name, address or Social Security Number. With new laws coming into play, there's a more fulsome definition of personal information that extends beyond NPPI to include geolocation information, IP addresses, email addresses and even any biometric information you might be collecting. These are some of the important considerations when laws like the CCPA start to encompass other categories of information within the definition of personal information.

For instance, consumers these days have come to expect the greatest convenience when executing a range of online financial transactions, whether they're using a laptop, tablet, mobile phone or other device. Security measures like facial recognition, biometrics, scanning, fingerprinting and eye scanning are now common, but remember that it's all considered personal information and comes with additional data management requirements. If you were collecting disparate pieces of information to create a profile and make business decisions vis-à-vis a client, it might also be viewed as personal information under various laws.

Although Europe is further along when it comes to consumer access to personal information, CCPA is helping Americans take a step forward. In mid-2020, California residents will be able to ask businesses to reveal what personal information they've collected, and those businesses will need to provide their response within a regulatory timeframe. Under these rules, businesses will be obligated to inform California residents about what specific categories of information they have gathered and whether that information has been sold or shared to anyone else.

Bear in mind, third parties provide services being offered to investors. These companies can range from marketing companies, to all types of service providers, including those involved in statement generation or firms supplying an investment model to investors. The new laws are putting more onus on the business to understand and map the lifecycle of that data – in a clear, consolidated inventory – to prove that they know where the data is going, how it's being used, how long it's being retained and ultimately how it's deleted.

Your opportunity to differentiate

Given the potential for severe fines and penalties for non-compliance, advisors should work with their lawyers to develop a defensible position on how they're handling data within the information lifecycle, especially in the event of security failures and breaches. All states have breach reporting requirements, but now CCPA is raising the bar and giving consumers/investors the right to take action. In fact, they can litigate, so there's an extra incentive for advisors and their firms to implement a locked-down process for knowing what information they're collecting, where it's being stored and how it's stored (e.g., file cabinets, systems applications, collaboration tools or even in emails). If you have employees who exchange HR information via email, you need to be aware of that because, whether it's through regulatory inquiry or an investor request, you're obliged to be in a position to provide a replay of the information you have stored.

Your ability to competently respond to those requests may increase the trust that you build with employees, investors and regulators alike. Other potential benefits of strong adherence to privacy legislation are financial, such as avoiding loss of revenue, litigation costs and remediation costs. Another benefit is the effective management of reputational risk. It often takes considerable time and effort to build a reputation, but you may lose it in the blink of an eye. You can avoid damage to your brand by keeping sensitive information secure and reducing your exposure to data breaches. A strong reputation for proficient data management can bolster client relationships. It can also be a valuable differentiator for your practice that can help sway client sentiment in your favor and become a tipping point for prospects trying to decide with whom to conduct their business.

Compliance is paramount because it helps you properly steward your clients' assets, and your reputation and personal brand are at stake as well. When you're compliant on data management issues, you avoid making negative media headlines and drawing regulatory scrutiny, whereas competitors may find themselves front and center if something goes awry and they are heavily penalized for a data breach. You can certainly do without this form of publicity, notably in the social media era of instant worldwide communication and judgement. It can be onerous to monitor, interpret and comply with privacy demands. Already a challenge for larger firms, smaller firms may find complexity and costs daunting. A RegTech strategy – using technology to help firms solve for regulatory and compliance issues – can be instrumental in helping firms of all sizes scale to regulatory demands and comply with new and existing regulations in an efficient, responsive manner.

Advisor best practices

When providing consultative services to our clients at Pershing, we discuss creating or refining a risk-based privacy program that considers all the aspects of data collection, and then taking those key concepts and trying to apply them broadly to a comprehensive data management process. Don't take a "wait and see" approach – you can gain a meaningful competitive advantage by being proactive rather than passive.

We don't recommend trying to comply only with current elements of a given state law, because you should be forward-looking. Instead of focusing on developing a program to comply with California law today, for instance, consider potential new laws in other states/jurisdictions and what nuances these laws may feature, including having different exemptions or different definitions of personal information.

> "Look at your privacy program and information security holistically to uncover common denominators across all laws (or potential laws). It's important to start with this perspective, then work to improve and mature your overall privacy program accordingly."
>
> *-Troy Guinn-Bailey*
> *Vice President, Privacy Compliance Officer at Pershing*

We typically advise our clients to set up a program that broadly applies and has the capacity to create a defensible position in the event of legal action. In addition to collaborating with your firm's legal counsel, try engaging experts who understand complex and evolving privacy regulations. Adopting a cross-functional approach involves performing a thorough analysis of your business and pulling in people from different areas of the organization, such as sales and marketing, data management, information security, compliance, executives and audit personnel, partnering with them from the start to ensure a holistic approach.

These professional functions play a critical role in testing and remediating issues. Together they can offer a robust perspective on the entire business and your data, helping you understand how you process data, whether you have a legal basis for retaining that data, and what is done with the data when you no longer have a contractual or regulatory basis for holding onto it. There could also be practices taking place within the firm that are bespoke and may warrant additional documentation and tailored oversight, and you wouldn't have been aware of them had you not consulted subject matter experts from around the firm to shed light on certain practices.

Be informed, be ready

Pershing is committed to educating advisors on the potential (and often significant) impact of industry regulations, helping them not only to prepare for regulatory change but to seize the opportunity as well. Our global team of experts has the resources and support capabilities to help advisors and their firms manage risk, achieve greater efficiency and drive growth – all while satisfying progressively stringent industry compliance requirements.

To help advisors and their firms navigate the ever-evolving landscape of data management and regulatory reform, we offer a robust educational program, including regulatory and compliance webcasts on various important topics that our legal and compliance teams

conduct roughly once a month. For instance, we may explore privacy regulation, provide a recap of CCPA, discuss upcoming regulatory change or take a look at data privacy laws across the globe. We also provide high-level overviews and FAQs through our marketing center that goes out through our NetX360® tool.

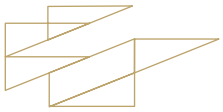
Tips for advisors in smaller firms

Because advisors in smaller firms lack the robust infrastructure, specialized resources and programs of larger organizations, they may need to be more hands-on with regulatory compliance.

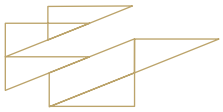
1. Privacy notices represent your policies and procedures. Make sure they're up to date and accurately reflect your practices.
2. If you're part of an affiliate and transfer sensitive information internally, disclose it in the privacy notice. Review and address individual rights processing because it's a fairly new concept.
3. When working with third parties, either those that supply data or those you may share data with, such as vendors or data processors, ensure contract language about data handling is fully compliant.
4. Examine how you exchange files with third parties to see if these files contain too much personal information for the task at hand.
5. If you transfer information outside America, disclose it and have the appropriate contracts and data protection safeguards in place.
6. Evaluate your firm's information security protocols to ensure they are current and have appropriate access and entitlement controls.

With our training and awareness materials, our goal is to provide clients with crucial updates and analysis of regulatory change. "We also share best practices among advisors and their firms," says Ken Shatzer, Vice President, Privacy Compliance at Pershing. "We have a constant finger on the pulse of the industry and are regularly involved in industry conversations about data protection and information security, and maintain a wide network of peers, clients and industry trade groups like the Securities Industry and Financial Markets Association to assist with benchmarking."

We conduct calls with our clients' compliance and operations personnel, so in addition to providing consultation services, we can also benchmark by discussing what actions we're taking relative to what our clients are doing.



The industry will inevitably continue to evolve, and data privacy issues and regulations will expand in scope. Advisors and their firms must stay at the forefront of this evolution and be ready to implement new policies, procedures and programs to keep pace. GDPR and the CCPA are just the tips of the regulatory iceberg, as we expect new laws to be implemented in the near future – not only around the world but also in our backyard as more states unveil their own reforms and the potential remains for a blanket federal privacy law.



Pershing

BNY Mellon's Pershing and its affiliates provide a comprehensive network of global financial business solutions to advisors, broker-dealers, family offices, hedge fund and '40 Act fund managers, registered investment advisor firms and wealth managers. Many of the world's most sophisticated and successful financial services firms rely on Pershing for clearing and custody; investment, wealth and retirement solutions; technology and enterprise data management; trading services; prime brokerage and business consulting. Pershing helps clients improve profitability and drive growth, create capacity and efficiency, attract and retain talent, and manage risk and regulation. With a network of offices worldwide, Pershing provides business-to-business solutions to clients representing approximately 7 million investor accounts globally. Pershing LLC (member FINRA, NYSE, SIPC) is a BNY Mellon company.

pershing.com

One Pershing Plaza, Jersey City, NJ 07399

WP-PER-WT-01-20