ICI OPERATIONS

OCTOBER 2021

Protecting Nonpublic Personal Information in a Data-Driven Distribution Model

Protecting Nonpublic Personal Information in a Data-Driven Distribution Model

Contents

Protecting Nonpublic Personal Information in a Data-Driven Distribution Model

Introduction

Distribution of mutual funds depends more on intermediaries today than ever before.[1] Intermediary distribution strategies often require the exchange of nonpublic personal information (NPPI)[2] between counterparties to meet important regulatory, compliance, oversight, and distribution needs—especially for mutual fund asset managers and their funds' boards of directors. Exchanging NPPI introduces numerous risks for all parties, including the shareholder or intermediary whose information is being shared, the counterparties that send and receive the data, and any entities serving as conduits for information exchange. Risks include unlawful or unnecessary cyber or employee access, constantly shifting regulation regarding NPPI management, and the legal and financial liabilities that could result from an NPPI data breach.

The Investment Company Institute's Broker-Dealer Advisory Committee (ICI BDAC) is committed to improving mutual fund distribution, operational processing, servicing, and support. ICI BDAC created its Data Strategy Task Force to understand how NPPI is shared between and used by mutual fund companies and counterparties such as intermediaries and service providers to support current distribution, shareholder servicing, and recordkeeping activities. This paper describes common practices and offers context and considerations for asset managers, intermediaries, and service providers regarding use and management of NPPI to support business activities such as regulatory and compliance management, intermediary oversight, distribution, and reporting.

The task force considered the following key questions to identify business use cases and practices using NPPI. The questions may be helpful to an organization as it evaluates its ongoing use and management of NPPI:

- What NPPI does your organization send to or receive from intermediaries and service providers?
- How and for what purpose is NPPI used?
- Are the uses and benefits of NPPI appropriate or necessary relative to the risks of transmitting, receiving, and/or storing such information?
- Can the business processes be supported through alternate means without NPPI, or through a lesser volume of NPPI?
- If NPPI is required, what action steps does/should your organization take to safeguard and protect NPPI while in transit or at rest within your organization, or while in the possession of your distribution partners and service providers?
- Are the safeguards and controls such as user provisioning, storage, retention, and destruction appropriate relative to regulations and the risk related to the NPPI data points?

---

1 Examples of intermediaries include broker-dealers; registered investment advisers (RIAs); bank/trust companies, including private wealth management organizations; recordkeepers for retirement plans, health savings accounts, and 529 qualified tuition plans; and insurance companies.

2 For the purposes of this discussion, NPPI includes 11 data points. Please refer to "Common Definition of Nonpublic Personal Information" on page 4 for details on how NPPI was identified for this paper.

» Considering your business model and shareholder base, what effect will/does regulation—including state consumer privacy laws such as the California Consumer Privacy Act (CCPA) or the European Union's General Data Protection Regulation (GDPR)—have on your use of NPPI?

Asset managers, intermediary partners, and service providers are encouraged to use this document as one resource to assess the extent to which NPPI is appropriately transmitted, received, stored, used, and disposed. Each organization will separately determine its internal information security policies and procedures, as well as applicable compliance and regulatory requirements. When possible, all parties are encouraged to remove unnecessary NPPI from their processes and environment, and reduce and protect required NPPI received from or provided to counterparties.

Background

Decades of growth in defined contribution retirement plans,[3] mutual fund supermarkets,[4] clearing arrangements,[5] managed account platforms,[6] and omnibus and super-omnibus models[7] has caused asset managers to become increasingly intermediated from the end investor. This shift has created numerous business challenges for asset managers that no longer have direct access to shareholder information for reporting and analytics. Asset managers and their fund boards are subject to extensive regulatory requirements that mandate the fund know pertinent information about all shareholders and related investment and shareholder servicing activities. Within a non-intermediated (often referred to as a "fund-direct") distribution model, asset managers could access shareholder information held directly by the fund's transfer agent (TA) to meet these obligations. For intermediated relationships, the same information is often only available through the intermediary's recordkeeping infrastructure.

The mutual fund industry responded to greater intermediation with data exchange solutions that provide transparency for asset managers and their service providers. The goal is to effectively support the asset manager's relevant business processes such as investor communication, distribution analytics, intermediary oversight, and regulatory reporting.

Many intermediaries using recordkeeping platforms provide shareholder account, transaction, and position information through industry standard solutions offered by the Depository Trust & Clearance Corporation (DTCC) Wealth Management Services, including its National Securities Clearing Corporation (NSCC) subsidiary's

[3] Examples include 401(k), 403(b), 457, and the Thrift Savings Plan.

[4] A mutual fund supermarket provides retail investors with access to a range of mutual fund products, often from multiple mutual fund companies, through one entry point (often referred to as a platform). Supermarkets may be offered by full-service or discount broker-dealers, who may offer the platform as part of an advice relationship with the shareholder.

[5] Clearing arrangements provide trade entry, clearance, and settlement technology and support to introducing intermediaries—such as a registered investment adviser—that typically works in an advice relationship with the shareholder.

[6] A managed account is an individual account owned by an institutional or retail shareholder, professionally managed by someone with discretionary authority that is hired by the shareholder, and may be made up of multiple securities and instruments.

[7] Omnibus accounts hold mutual fund shares that are registered with the mutual fund's transfer agent in the name of the financial intermediary. The intermediary maintains the underlying shareholder (beneficial owner) account information on its own subaccounting or retirement plan participant recordkeeping systems and reports share transactions to the funds on an aggregate basis. The intermediary or its agent handles all communications and servicing of its customer accounts. Super-omnibus accounts hold multiple omnibus accounts as primary shareholders.

Fund/SERV® and Networking, DTCC Payment aXis®, and especially Omni/SERV®.[8] ICI BDAC sponsored the creation of Omni/SERV in 2009 to standardize transmission of existing Data Share Activity (DSA), Data Share Position (DSP), and 529 Plan master aggregation files that provide asset managers with underlying shareholder account transparency for omnibus relationships. There is strong consensus across the industry for asset managers, intermediaries, and service providers to leverage DTCC's secure infrastructure, when possible, to share NPPI and reduce the risk of data breach during transmission, all while gaining operational efficiencies through transmission standardization. Omni/SERV has been broadly adopted by traditional and clearing broker-dealers; there are opportunities to increase adoption in other intermediary arrangements.

Asset managers and their intermediary partners may use supplemental files and reports containing NPPI to support various business processes. Task force members indicate that most are transmitted through secure and encrypted connections. For example, some industry participants use DTCC Payment aXis to transmit fee information related to SEC Rule 12b-1, service fees, and contingent deferred sales charges (CDSCs). In other cases, files and reports containing NPPI may be transmitted directly between two parties (referred to as "point-to-point" connections) with varying levels of information security and encryption.

The Risk of NPPI Data Breach

While asset managers, intermediaries, and service providers often use secure and encrypted transmission protocols through DTCC or point-to-point connections, the risk of an NPPI data breach through other means remains a concern for entities managing NPPI, due to many factors:

» Increasing global cybersecurity threats perpetrated by bad actors

» Growing volume of NPPI shared as regulatory and oversight needs evolve

» Adding additional or redundant NPPI to an increasing number of "standalone" sources (e.g., files, reports) used for existing processes

» Expanding complex and, sometimes conflicting, international, federal, and state regulatory requirements, including opt-out provisions governing NPPI management, use, and disposal

» Evolving shareholder privacy expectations

» Broadening use of data analytics and underlying NPPI for business decision making

» Increasing role of third parties receiving, managing, and using NPPI

» Expanding use of DSA and DSP files as a data source for processes where NPPI is not required

» Maintaining or introducing products and reporting requirements that depend on NPPI

[8] DTCC's Wealth Management Services—Mutual Fund Services business unit serves as the industry's utility supporting important trading, clearance, and settlement of mutual fund share transactions; it also facilitates information sharing among trading counterparties to meet a host of operational and regulatory needs. Refer to www.dtcc.com/wealth-management-services/mutual-fund-services for more information.

Scope and Methodology

The task force pursued a multifaceted, data-driven strategy to develop this paper. The task force first agreed that its focus would be on the back-office distribution, servicing, and support of mutual fund and 529 plan products. Next, the task force drew upon each member organization's own definition of NPPI to formulate a consensus-based definition to guide the task force's efforts. As background, the task force also documented a high-level information flow of when and how NPPI is passed between counterparties. ICI BDAC members provided the task force with their inventory of industry standard and nonstandard files, reports, and other tools for electronic data exchange, and the task force compiled the data elements from each that could be considered—alone or in some combination—as conveying NPPI. The task force also solicited input from ICI BDAC on the many business use cases supported by the inventory. Each business case was aggregated by topic, catalogued, and reviewed by the task force regarding NPPI use, including review of any alternative approaches that did not rely on NPPI.

This paper is a result of that review and analysis. It provides context and offers a framework for an organization to inventory its business processes, including assessment of when and how NPPI is used. An organization can make informed decisions regarding NPPI use and determine whether it is possible to implement alternative processes that reduce or eliminate dependence on NPPI. The paper includes considerations for implementing such changes, as well as considerations for governance and oversight where NPPI continues to be used.

Common Definition of Nonpublic Personal Information

Task force members provided their unique definition of NPPI and used this information, along with a review of sample data files and reports, to develop this paper's definition of NPPI. The definition includes data elements that alone or in combination constitute NPPI.

Nonpublic personal information (NPPI). NPPI is generally defined as restricted information that, if improperly accessed, disclosed, used, altered, or destroyed, would result in regulatory, reputational, financial, or legal liability to an organization or its clients, or would cause a materially adverse impact to an organization, its business partners, or clients. The definition covers data while in transit or at rest in applications, databases, and systems, and may have been produced or retained in electronic or hard copy.

FIGURE 1

Elements of Nonpublic Personal Information

Data point	Definition
Account number	The main identifier of a shareholder's positions and activity in a recordkeeping system
Broker Identification Number (BIN)	The main identifier of a shareholder's positions and activity in a brokerage (intermediary) system; a BIN may be associated with multiple products and investment vehicles such as mutual funds, equities, bonds, and options
Owner name	The legal owner(s) of an account; the first and last name of a person or persons or the name of a nonperson (e.g., organization, corporation, trust)
Owner address	The street address, city, state (province), ZIP (postal) code, and country of the account owner(s)
Owner Tax Identification Number (TIN), Social Security Number (SSN), or Employee ID Number	Government-issued identification number assigned to the legal owner(s) of an account
Branch Identification Number	A value used to designate the intermediary or broker-dealer branch where an account representative conducts business
Account representative number	A value used to identify the individual or team of financial advisers or representatives assigned to an account or associated with a transaction
Account representative name	The name(s) of the financial adviser(s) or representative(s) assigned to an account
Beneficiary name	The first and last name of the beneficiary of an account
Beneficiary TIN or SSN	Government-issued identification number assigned to an account beneficiary
Beneficiary or successor owner date of birth	The date of birth of the beneficiary or successor owner of an account

In some instances, any one data point may not, in and of itself, constitute NPPI; rather, it is the combination of data points available while in transit or at rest that can create NPPI.

High-Level Information Flow

In the intermediary-distributed business model, a shareholder will establish an account with their broker-dealer, adviser, bank, trust company, or plan provider (e.g., retirement, health savings, 529). The shareholder must provide certain NPPI such as name, address, and TIN or SSN when opening the account. They provide that NPPI with the expectation that it will be protected, used, and shared with third parties for bona fide business purposes only.

When a shareholder places a mutual fund financial transaction, transaction information including certain NPPI is shared by the intermediary with the asset manager or its transfer agent. The flow of NPPI from the intermediary to the asset manager depends on the operating model. The following addresses the two most common intermediary-centric recordkeeping models: (1) an individual account model,[9] and (2) an omnibus account model.

In most non-omnibus (individual account) recordkeeping models, NPPI is transmitted by the intermediary to the mutual fund transfer agent through DTCC Fund/SERV and Networking. Far less frequently, NPPI also may be transmitted via proprietary interface (e.g., file transmission or web portal) or through paper documents by mail or facsimile. All relevant shareholder account and transaction information is retained by the mutual fund transfer agent. Conversely, the transfer agent transmits DTCC Fund/SERV, Networking, and Payment aXis files containing shareholder NPPI to the intermediary or its service provider. The transfer agent may also deliver files, reports, or documents such as transaction confirmations, statements, and tax forms that may contain NPPI. The mutual fund transfer agent will also transmit relevant information including NPPI to the asset manager, third-party partners such as 529 plan sponsors, and the fund's service providers such as sales reporting, proxy, or blue sky vendors. Other than the sharing of NPPI between intermediary and fund transfer agent, these models work in a similar fashion as if the shareholder opened an account directly with the fund's transfer agent (i.e., the fund-direct distribution model).

In an omnibus recordkeeping model, aggregate trades that may be applicable to multiple underlying shareholders are sent by the intermediary or its subaccounting/recordkeeping service provider to the mutual fund transfer agent. Trading may occur through DTCC Fund/SERV or other means. In traditional broker-dealer intermediary arrangements, the intermediary or its subaccounting service provider transmits shareholder NPPI, transaction activity, and position information on a post-execution basis to the asset manager or the asset manager's third-party partners and service providers. These files may be transmitted through DTCC Omni/SERV, through proprietary file structures and networks, or via a point-to-point connection.

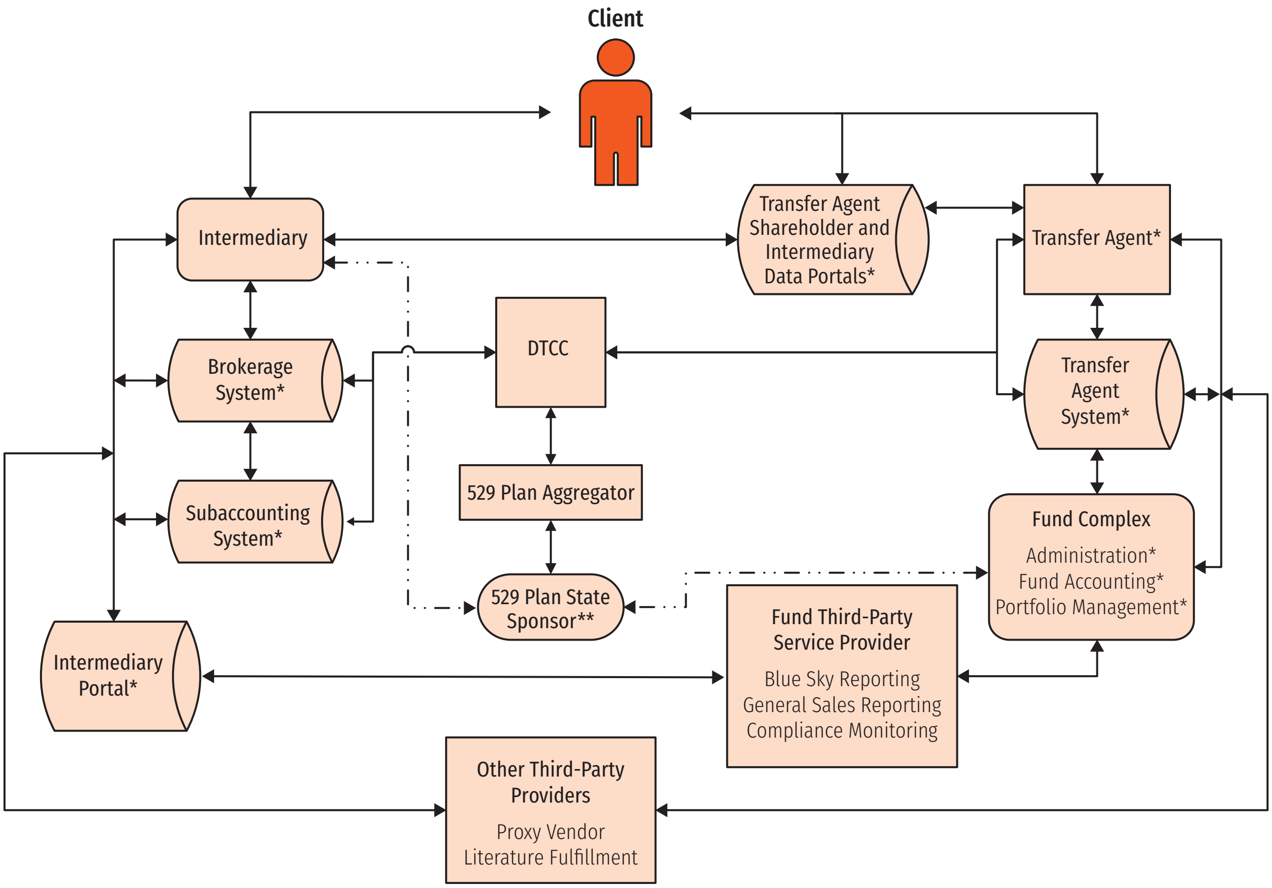
While individual practices may vary, shareholder information, transaction activity, and positions may also be made available through an intermediary, asset manager, or transfer agent portal or website. Access typically occurs through an encrypted file transmission or by a secure application programming interface (API).

Please refer to the following schema that graphically illustrates the various ways that NPPI may be exchanged within the mutual fund back-office trading ecosystem between asset managers, intermediaries, and related service providers.

[9] Prior to the rise of the omnibus model, it was common practice for intermediaries to establish individual broker-controlled accounts with the fund's transfer agent for each of their customers. The accounts were registered with reference to the name of the shareholder or the BIN issued to the shareholder by the broker-dealer, and all transaction activity and instructions related to the account originated with the broker-dealer on behalf of the shareholder.

FIGURE 2

Potential NPPI Data Flows in Mutual Fund Back-Office Operations



* Entities or the systems provided may be considered internal to the organization, or may be provided by a third party.

** An *Intermediary* **or** *Fund Complex* that serves as a 529 Plan Program Manager will typically have reporting requirements with its respective state plan(s).

File and Report Inventory

Communication of NPPI between counterparties is typically accomplished through data files and reports. Figure 3 provides a brief description of the most common files, their uses and transmission methods, suppliers, recipients, and consumers. In some instances, the recipient may act as a conduit and transmit the file to a third-party service provider. While some of these files support just one or a few related processes, the omnibus DSA and DSP files that typically include the greatest volume of NPPI are used to support multiple unrelated business processes.

FIGURE 3

Distribution-Related Files/Reports Used by Mutual Fund Back-Office Operations

File/Report	Description	Uses	Transmission methods	Suppliers	Recipients	Consumers
529 plan master aggregation	529 plan shareholder registration and summary contributions/transactions	» 529 plan rules enforcement » Regulatory reporting	» NSCC Omni/SERV » Point-to-point	» Intermediary » Recordkeeper » TA » Master aggregator	» Intermediary » Recordkeeper » TA » Master aggregator	» Intermediary » Recordkeeper » TA » Master aggregator
Blue sky	Mutual fund share sales data reported by state of sale and/or social code	» Regulatory reporting	» Point-to-point	» Intermediary » Recordkeeper » TA	» TA » Blue sky service provider	» Blue sky service provider
CDSC[10] liability and remittance	Collected CDSC and outstanding liability associated with an omnibus account and reported by shareholder account number, BIN, and transaction	» Fee reporting » Fee invoicing » Compensation	» DTCC Payment aXis » Point-to-point » Email	» Intermediary » Recordkeeper » TA	» TA » Asset manager » Fund service provider	» TA » Asset manager » Fund service provider
Dealer resignations	Funds deliver file of dealer-associated accounts from the fund's TA Intermediaries deliver instructions to resign as broker-dealer from fund TA accounts	» Transaction processing	» NSCC Networking » Email » Mail » Fax	» Intermediary » Recordkeeper	» TA » Asset manager	» TA » Asset manager
DSA (Omnibus Data Share Activity)	Intermediary-initiated activity reported by shareholder position	» Sales reporting » Omnibus oversight » Regulatory reporting	» NSCC Omni/SERV » Point-to-point	» Intermediary » Recordkeeper	» TA » Asset manager » Fund service provider	» Asset manager » Fund service provider
DSP (Omnibus Data Share Position)	Intermediary-reported shareholder position balances	» Sales reporting » Omnibus oversight » Regulatory reporting	» NSCC Omni/SERV » Point-to-point	» Intermediary » Recordkeeper	» TA » Asset manager » Fund service provider	» Asset manager » Fund service provider
Fund/SERV transaction order confirmations	Buy/sell/exchange mutual fund share confirmations	» Transaction processing	» NSCC Fund/SERV » NSCC Networking » Point-to-point	» TA » Recordkeeper	» Intermediary » Recordkeeper	» Intermediary » Recordkeeper
Fund/SERV transaction orders and account registrations	Buy/sell/exchange mutual fund shares; establish new accounts	» Account setup » Transaction processing	» NSCC Fund/SERV » Point-to-point	» Intermediary	» TA » Recordkeeper	» TA » Recordkeeper

10 A CDSC (Contingent Deferred Sales Charge) is paid on the sale of shares held in certain share classes, as described in the fund prospectus, when the required share retention period prior to sale has not been fulfilled.

FIGURE 3, CONTINUED

Distribution-Related Files/Reports Used by Mutual Fund Back-Office Operations

File/Report	Description	Uses	Transmission methods	Suppliers	Recipients	Consumers
Networking new account maintenance and transfers	Account registration and maintenance; share transfers	» Account setup » Account updates » Transaction processing	» NSCC Networking » Point-to-point	» Intermediary	» TA » Recordkeeper	» TA » Recordkeeper
Networking activity and reconciliation	Account activity, dividend, and positions	» Reporting fund-initiated activity » Reconciliation	» NSCC Networking » Point-to-point	» TA » Recordkeeper	» Intermediary » Recordkeeper	» Intermediary » Recordkeeper
Proxy and fulfillment	Shareholder demographic and share balance information	» Fulfillment » Regulatory requirement	» Point-to-point	» Intermediary » Recordkeeper » TA	» Asset manager » Fund service provider	» Asset manager » Fund service provider
Rights of accumulation (ROA) and letter/statement of intent (LOI/SOI)	Volume- or agreement-related sales charge reductions reported by shareholder account number or BIN	» Breakpoint analysis	» Point-to-point	» TA » Recordkeeper	» Intermediary » Recordkeeper	» Intermediary » Recordkeeper
SEC Rule 12b-1 fee invoices	12b-1 fees associated with an omnibus account reported by shareholder account number or BIN	» Fee reporting » Fee invoicing » Compensation	» DTCC Payment aXis » Point-to-point » Email	» Intermediary » Recordkeeper	» TA » Asset manager » Fund service provider	» Asset manager » Fund service provider
SEC Rule 22c-2 compliance	Transaction activity associated with a shareholder account, BIN, or TIN/SSN	» Regulatory reporting	» NSCC Networking » NSCC Omni/SERV » Point-to-point	» Intermediary » Recordkeeper » TA	» TA » 22c-2 service provider	» TA » 22c-2 service provider
Service fee invoices	Service fees associated with an omnibus account reported by shareholder account number or BIN	» Fee reporting » Fee invoicing » Compensation	» DTCC Payment aXis » Point-to-point » Email	» Intermediary » Recordkeeper	» TA » Asset manager » Fund service provider	» Asset manager » Fund service provider
Supplemental sales reporting	Supplemental shareholder activity and balance information from an intermediary's recordkeeping system	» Sales reporting	» Point-to-point	» Intermediary » Recordkeeper	» TA » Asset manager » Fund service provider	» Asset manager » Fund service provider
Transfer agent portals and proprietary files	Information on direct accounts held with the transfer agent but associated with the intermediary	» Reporting fund-initiated activity » Regulatory compliance » Reconciliation	» Point-to-point	» TA	» Intermediary	» Intermediary
Underwriter commission	Underwriter commission associated with an omnibus account and reported by shareholder account number, BIN, and transaction	» Fee reporting » Fee invoicing » Compensation	» DTCC Payment aXis » Point-to-point » Email	» Intermediary » Recordkeeper » TA	» TA » Asset manager » Fund service provider	» TA » Asset manager » Fund service provider

NPPI Use Cases

Based on information provided by the ICI BDAC, the task force identified various use cases where information is shared between asset managers, intermediaries, and service providers. In each use case, at least one data element defined by the task force as NPPI is included. In most use cases, DTCC Fund/SERV, Networking, and the DSA and DSP are used as the exclusive or primary information sources. The master aggregation file is used to support 529 plan reporting. Other use cases leverage less commonly used or nonstandard files and reports transmitted between counterparties via various transmission methods.

The task force created three components that, when used together, provide information regarding common industry use cases.

» Use case definition

» Primary and secondary source data for each use case

» Key NPPI and other data points relevant to each use case

Task force members have indicated the utility of these components as they identify their organization's use cases. Following a definition of each use case and its purpose, two tables present typical data source(s) and key NPPI and non-NPPI data points by use case name, listed in alphabetical order.

Use Case Definitions

1. **Best pricing:** Intermediaries, asset managers, and their service providers may populate a data repository with daily shareholder activity and position data, typically from the DSA and DSP, to apply ROA or SOI/LOI for best pricing. Accounts are typically linked by a combination of fund account number, BIN, TIN, or a separate group indicator.
2. **Blue sky operations and reporting:** Asset managers or their service providers use aggregate blue sky sales reporting files to identify reportable sales for each state and to apply exclusions and exemptions. These sales contribute to required blue sky permit reporting and filing. The transfer of NPPI most commonly occurs when research is necessary regarding state-reported violations or "overselling" shares filed for sale.
3. **CDSC and underwriter commission reporting:** In omnibus arrangements, the intermediary collects CDSC and other fees because the asset manager does not have sufficient information to determine CDSC liability. The intermediary or its subaccounting service provider calculates these fees and may provide related shareholder information to the asset manager.
4. **Corporate tax reporting:** Asset managers are subject to tax obligations based on shareholder domicile. States typically require each fund to report the number of shareholders and revenues from income generated by assets of direct and indirect fund shareholders domiciled within their respective states, and in some cases localities such as cities, boroughs, and counties.

5. **Direct account reporting (fund to intermediary):** Intermediaries monitor direct accounts held with the mutual fund transfer agent for which they are named as broker-dealers, in response to SEC Regulation Best Interest and Financial Industry Regulatory Authority (FINRA) requirements.[11] The transfer agent typically uses NSCC Networking or another format to provide the intermediary or its service provider with its direct accounts to review. In some instances, the intermediary may instruct the asset manager or its transfer agent to remove it as dealer of record where a relationship with the shareholder no longer exists. This process requires NPPI to be shared between the asset manager and intermediary.
6. **Fee and compensation eligibility:** Asset managers may apply exclusions or adjustments when paying SEC Rule 12b-1 fees, service fees, or other fees and compensation to intermediary and trading platform partners. DSA and DSP file data points are often used to determine exclusions that are guided by the prospectus, distribution agreement, or other regulatory requirements.
7. **529 plan master aggregation (intermediary to fund and fund to intermediary):** Various federal and state regulations require 529 plans to monitor, remediate, and report on certain owner and beneficiary activities across all accounts held within a state's various 529 plans.[12] The master aggregation process allows the entities that service 529 plans to exchange information, including shareholder NPPI, to support these processes.
8. **529 plan state reporting:** Certain states require 529 plan managers (asset managers or intermediaries) to provide owner and beneficiary data. This information is used for scholarship and other state reporting purposes. The information collected varies by state.
9. **Foreign account monitoring:** Asset managers may prohibit investments by nonresident aliens, US citizens living abroad, or foreign investors. Asset managers monitor for and remediate prohibited investments.
10. **Money market fund product eligibility:** To comply with money market definitions of retail versus institutional investors for product eligibility, asset managers must evaluate purchase activity to ensure that only eligible shareholders are investing in the money market fund. Additional NPPI may be provided when non-NPPI data are insufficient to determine eligibility.
11. **Omnibus oversight:** Asset managers must ensure that fund prospectus rules are applied fairly to all shareholders, including those serviced by intermediaries. This responsibility includes, but is not limited to, determination of share class eligibility, application of purchase minimums, sales loads, and applicable waivers (e.g., CDSC, other fees). Asset managers may use account number, BIN, or TIN to identify a shareholder or account.
12. **Order trade processing:** Intermediaries submit shareholder or omnibus trades to the fund's transfer agent through DTCC Fund/SERV or proprietary formats. For shareholder trades, account registration information is required to establish the account on the fund's transfer agency system. The extent to which NPPI is shared, especially related to individual shareholder activity, is determined by the asset manager and each intermediary partner and, for NSCC-traded accounts, varies depending on the Networking level and level of disclosure.[13]

---

[11] Refer to SEC final rulemaking "Regulation Best Interest: The Broker-Dealer Standard of Conduct." Available at www.sec.gov/rules/final/2019/34-86031.pdf. Refer to FINRA Regulatory Notice 11-02, January 2011 regarding Rule 2090 (Know Your Customer) and Rule 2111 (Suitability). Available at www.finra.org/sites/default/files/NoticeDocument/p122778.pdf.

[12] For example, many states offer both direct-sold (to shareholders) and adviser-sold (to shareholders through an intermediary) 529 plans. Federal and state regulations require lifetime contribution limits and annual strategy changes for the same owner across all state plan accounts to be monitored and, when exceeded, remediated. In addition, owner and beneficiary cost and earnings must be reported across all plan accounts within the same state.

[13] Networking level 4 accounts are comanaged by the fund's transfer agent and intermediary and tend to disclose full shareholder name and address information. Networking level 3 accounts are broker-controlled, and the registration typically does not reference the individual shareholder's name and address.

13. **Ownership reporting:** Asset managers are required to provide information related to certain fund shareholders to their fund boards and regulators. These shareholders may include investors who hold a certain percentage of the fund's total assets, or foreign investors, as required by federal or state regulation. Because a shareholder may hold a fund with multiple intermediaries, asset managers often use TIN to gain an aggregate view of ownership.
14. **Proxy and literature fulfillment (intermediary to service provider):** Intermediaries provide separate shareholder information files to the asset manager or a third-party service provider to meet fulfillment, proxy mailing, and related tracking obligations. Due to the fact that these materials are mailed or otherwise delivered to shareholders, NPPI such as shareholder name and address is included in these files. Some intermediaries providing fully disclosed shareholder information on DSA files may use the DSA to meet this need.
15. **Retirement asset tracking and reporting:** Asset managers have certain distribution, compliance, regulatory, and operational reporting requirements associated with their retirement plan platform partners. Asset managers may use account number, BIN, or TIN to identify a shareholder or account.
16. **SEC Rule 22c-2 compliance:** Asset managers or their service providers evaluate shareholder trading activity and identify and remediate instances where transactions violate the fund's short-term trading policies described in the prospectus. Some asset managers use shareholder TIN, while others use BIN or other supplemental information to identify related activity. Using account number or BIN for this process may limit the asset manager's ability to detect shareholders that are attempting to circumvent frequent trading policies by trading across accounts or broker-dealers.

FIGURE 4

Use Case Source Data

Use case	Primary source/files	Secondary source/files
1. 529 plan master aggregation	» 529 plan master aggregation	
2. 529 plan state reporting	» 529 plan master aggregation	
3. Best pricing	» DSA » DSP	» Networking activity and reconciliation—direct account Networking
4. Blue sky	» Blue sky (service provider—proprietary)	» DSA, DSP
5. CDSC and underwriter	» CDSC liability » Underwriter commission	» DTCC Payment aXis
6. Corporate tax reporting	» DSP	
7. Direct account reporting	» Daily networking activity and reconciliation » Transfer agent portals and proprietary files	» Networking activity and reconciliation—direct account Networking
8. Fee and compensation eligibility	» DSA » DSP	» SEC Rule 12b-1 fee invoices » Service fee invoices » Supplemental sales reporting
9. Foreign account monitoring	» DSA » DSP	
10. Money market fund product eligibility	» DSA » DSP	» Supplemental sales reporting, including trade and registration data
11. Omnibus oversight	» DSA » DSP	
12. Order trade processing	» NSCC Fund/SERV » NSCC Networking	» Proprietary trading networks/files
13. Ownership reporting	» DSP	
14. Proxy and literature fulfillment	» DSP	
15. Retirement asset reporting and tracking	» DSA » DSP	» Supplemental sales reporting
16. SEC Rule 22c-2 compliance	» DSA » DSP » NSCC Networking Standardized Data Reporting	» Proprietary recordkeeper files

FIGURE 5

Use Case Supporting Data Points

	NPPI							Other data				
Use case	Fund account number	BIN	Account owner	Full address	Partial address	TIN	Branch/ Rep.	CUSIP	Social code	Share balance and account value	Transaction amount	Other
1. 529 plan master aggregation	X	X	X	X		X		X	X	X		
2. 529 plan state reporting	X	X	X	X		X		X	X	X		
3. Best pricing	X	X				X	X	X	X	X		» Dealer concession
4. Blue sky		X	X		X			X	X	X	X	» Blue sky state of sale
5. CDSC and underwriter		X						X		X	X	» Other transaction details
6. Corporate tax reporting					X			X	X	X		
7. Direct account reporting	X	X	X	X		X	X	X	X	X	X	
8. Fee and compensation eligibility	X	X					X	X	X	X		» Program ID
9. Foreignaccount monitoring	X	X			X			X				
10. Money market fund product eligibility	X	X	X					X	X			
11. Omnibus oversight	X	X				X		X	X	X	X	
12. Order trade processing	X	X	X	X		X	X	X	X	X	X	» Program ID » Consultant
13. Ownership reporting	X	X				X		X		X		
14. Proxy and literature fulfillment	X	X	X	X				X				
15. Retirement asset tracking and reporting	X	X	X				X	X	X	X	X	» Program ID » Consultant
16. SEC Rule 22c-2 compliance	X	X				X	X	X	X	X	X	» Program ID » Consultant

Questions and Considerations

With an understanding of how NPPI flows between intermediaries, asset managers, and service providers, an organization is positioned to take the following steps:

1. Inventory and evaluate business processes and controls where NPPI is involved.
2. Consider whether a viable alternative with lesser or no NPPI dependency may meet the business need, and, if yes, determine if and when the alternative could be implemented.
3. If NPPI must remain involved in a business process, assess the controls, oversight, and governance practices in place and confirm that they are appropriate and consistent with the organization's information security risk management program.

Business Process and NPPI Inventory

Task force members stress that taking an inventory of business processes and NPPI related to the intermediated distribution of mutual funds is an important first step toward making sound decisions regarding NPPI practices (e.g., delivery, receipt, storage, use, and destruction). The task force identified the following items to catalogue:

» Business process name

» Brief description of the business process

» Assessment of the overall suitability of the method to transmit or access NPPI

» Where the business process is executed: internally, externally by a third party of your selection, or externally by a distribution partner or a third party of the distribution partner's selection

» Your organization's role in the business process: as information provider, process executor, information recipient, or multiple roles (e.g., as a conduit, serving as information recipient and provider)

» Names of the entities providing NPPI as an input into the business process

» Names of the entities receiving NPPI used as an input into the business process

» Your organization's relationship to the NPPI providers and recipients

» Names of the entities providing NPPI generated as output from the business process and your organization's relationship to the entities

» NPPI elements received and used as an input into or output from the business process

» NPPI elements received and not used as input into or output from the business process

» The manner of storage, retention, safeguarding, and destruction of NPPI related to the business process

It is important to recognize that NPPI may be provided directly to an organization's service provider. For example, some intermediary recordkeeper technology providers deliver NPPI directly to a proxy and fulfillment service provider. In such instances, organizations using service providers should consider this NPPI as under their responsibility.

The format and manner in which an organization delivers, grants access to, receives, or accesses NPPI should also be part of this inventory. For example, an organization may grant or obtain access to shareholder NPPI through a portal, file transmission, API, secure email, or hard copy format (e.g., an account application).

Business Process and NPPI Analysis and Action

Using the business process inventory, an organization can complete an assessment of the delivery, receipt, and use of NPPI. The first step is to determine whether the transmission, storage, retention, and access methods employed by an organization and its service providers are appropriate. This determination will be governed by an organization's information security policies and procedures. Considerations may include the following:

» Does each transmission/access method comply with the organization's information security policies and procedures?

» Do the storage, retention, and provisioning practices comply with the organization's information security policies and procedures?

» Are there controls and policies in place to prevent the erroneous or inappropriate dissemination of NPPI?

» Are there controls and policies in place to prevent non-secure transmissions?

» Are there provisioning controls in place to prevent unauthorized access to NPPI?

An organization may wish to further inventory the NPPI in its possession and in the possession of its service providers and determine whether the NPPI received is needed. Considerations may include the following:

» What NPPI does the organization or service provider receive that does not support business processes?

» When NPPI is used to support a business activity, is there a reasonable alternative (e.g., non-NPPI data—single or multiple data points) that may allow for the reduction or removal of NPPI?

» How can the organization engage with distribution counterparties and service providers to remove or reduce the presence of unnecessary NPPI?

» Is NPPI stored, retained, and disposed of in accordance with the organization's information security policies and procedures?

There may be instances where a file or report containing NPPI serves as an input into a business process, but one or more of the NPPI elements contained within the file or report are not required to execute the business process. For example, many intermediaries provide a shareholder's full name, address, and TIN through Fund/SERV and Networking or through the DSA or DSP files. An organization may determine that one or more of these NPPI elements are not required to support its business processes. In such cases, an organization should consider requesting that the intermediary remove NPPI from the file or report. If the NPPI cannot be removed from a file or report, the recipient should take special care to provision access and destroy NPPI that is not needed.

An organization's assessment may determine that NPPI elements are currently used in a process, but a reasonable non-NPPI alternative exists. Determining whether a reasonable alternative exists may include assessing the relative risk of the current and alternative processes, including the risk associated with being in possession of NPPI. For example, could a business process that uses full shareholder address (accessible on several legacy files through DTCC and DSA/DSP) be modified to use only postal ZIP code?

When modifying a process, care must be taken to ensure that the new process still meets its business objective. This may require coordination with internal stakeholders and service providers to ensure that systems and processes are in place to execute the new process. These changes may require systems modifications, testing and validation of results, and updated policies and procedures. Similarly, care must be taken to work with distribution partners or service providers that are providing the data.

In all cases, any unneeded NPPI should be removed from the business process as far upstream as possible. For example, if an organization determines that NPPI may be removed from DTCC Fund/SERV, Networking, or the DSA and DSP files, they may elect to work with distribution partners to determine if the NPPI elements can be removed from the files. If the NPPI elements are required for some, but not all business processes supported by these files, the receiving organization may elect to control access to the NPPI element through access provisioning.[14]

Another way to reduce NPPI is to identify where more than one data source could provide the necessary NPPI for two distinct business processes. For instance, SSN may be deemed essential NPPI for two processes, and therefore be sourced from two different places. If all SSN information could come from one source, it may be possible to eliminate the second data source—or at least eliminate SSN from it—and reduce the number of NPPI-related future storage, retention, and provisioning considerations.

Given the large number of relationships between intermediaries, asset managers, and service providers, the time and effort required to enhance business processes, remove unneeded NPPI elements from files, and update transmission methods may be considerable. An organization may elect to prioritize these efforts based on the relative risks associated with the current processes and methods, and the benefit or effect of changes.

[14] Access provisioning broadly describes the controls applied or permissions granted to people or machines when interacting with various data files, reports, and portals. For instance, access provisioning may limit system or human access to a data file, or it may mask or encrypt certain data points based on the security/access authority of the system or person accessing the data file.

Oversight, Governance, and Risk Management

For many industry participants, the business processes associated with distribution of mutual funds are complex. Many processes such as transfer agency, subaccounting, sales reporting, and blue sky reporting are outsourced to third parties or depend upon clients or distribution partners providing data that include NPPI.

When assessing these relationships, an organization may elect to determine the risk profile of each distribution partner and service provider.

- » How significant is the relationship in terms of key metrics such as number of shareholders, accounts, and assets?
- » How well do the partner's information security policies, procedures, and practices align with the organization?
- » Does a partner process NPPI internally or outsource the work to a third party?

It is also important for an organization to understand the mechanisms and controls currently in place to oversee the activities performed by distribution partners or service providers.

- » Are the terms in contractual agreements that govern information security and the use of NPPI appropriate?
- » What are the criteria for reviewing audit reports and attestations?
- » Are the due diligence activities that an organization employs effective and appropriate?

When an issue or concern is identified, it is important to have open communication with distribution partners and/or service providers, and to take appropriate steps to address any concerns and mitigate any risks. Many organizations have staff dedicated to intermediary oversight, third-party vendor/supplier management, and information security. Each organization should consider how to best engage and leverage personnel in conjunction with technology to ensure that the creation, distribution, use, and destruction of NPPI in the ecosystem described within this document are appropriately addressed in line with the organization's information security practices.

Summary and Conclusion

The operational environment supporting the distribution of mutual funds is complex and continues to evolve. There are many participants, including intermediaries and their recordkeepers, asset managers and their transfer agents, and third-party technology and business solutions service providers that support important activities in fund operations. This complex ecosystem sometimes requires NPPI to be shared. While the processes and methods to manage NPPI used by industry participants are mature and effective, there is a need to continually assess where, how, and why NPPI is used. Taking opportunities to reduce reliance on NPPI and eliminate instances where it is needed, when possible, will go far to reduce operational risk in shareholder servicing. Ultimately, both individual organizations and the broader mutual fund industry are charged with effectively transmitting, receiving, storing, using, and disposing of shareholders' NPPI. Doing so will help the industry retain the trust that more than 100 million investors have placed in it to help them achieve long-term financial goals through investing in the capital markets.