NOVEMBER 2021

DATA RISKS AND BEST PRACTICES: OBSERVATIONS FROM DTCC'S INSURANCE & RETIREMENT SERVICES (I&RS) BUSINESS

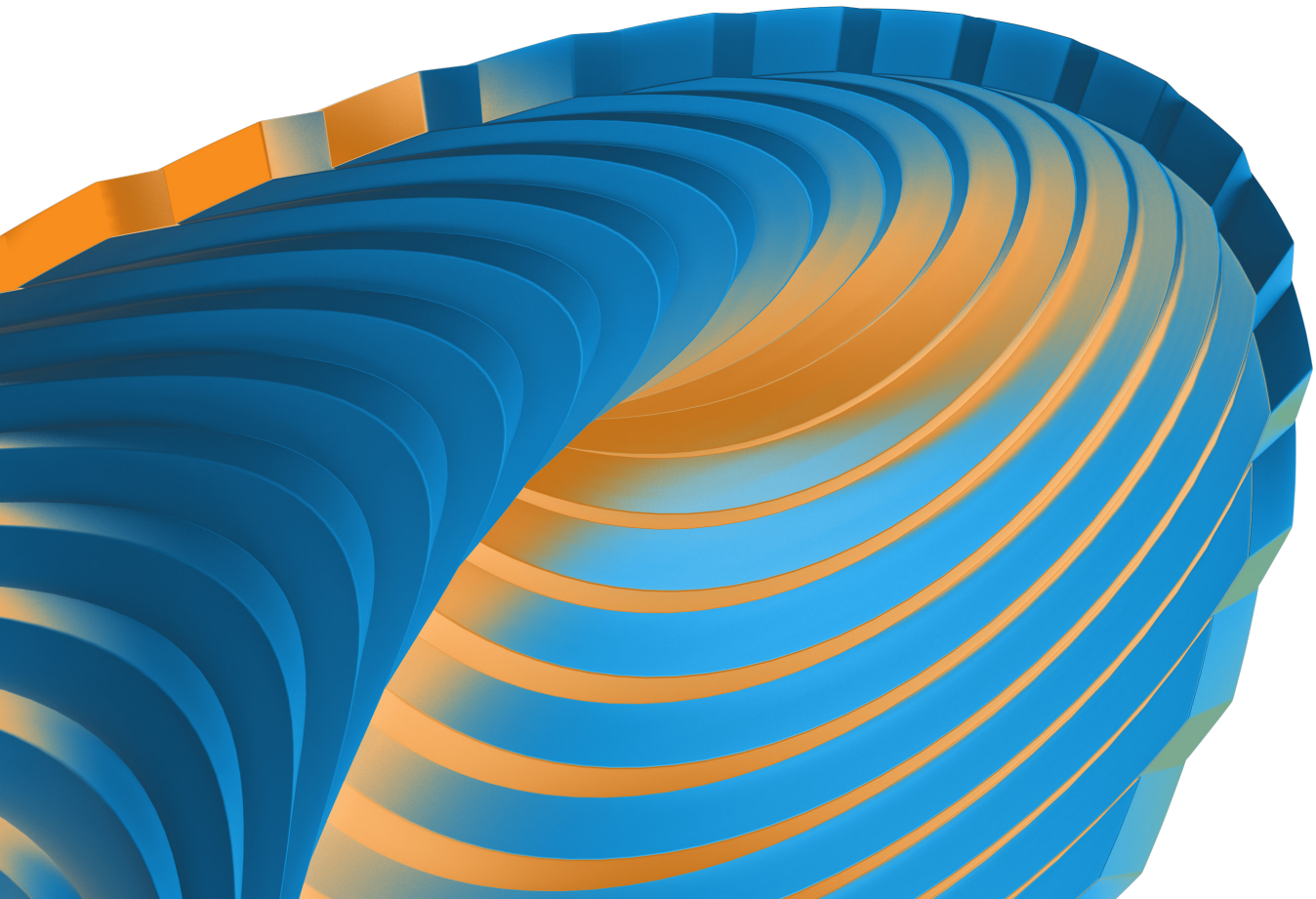
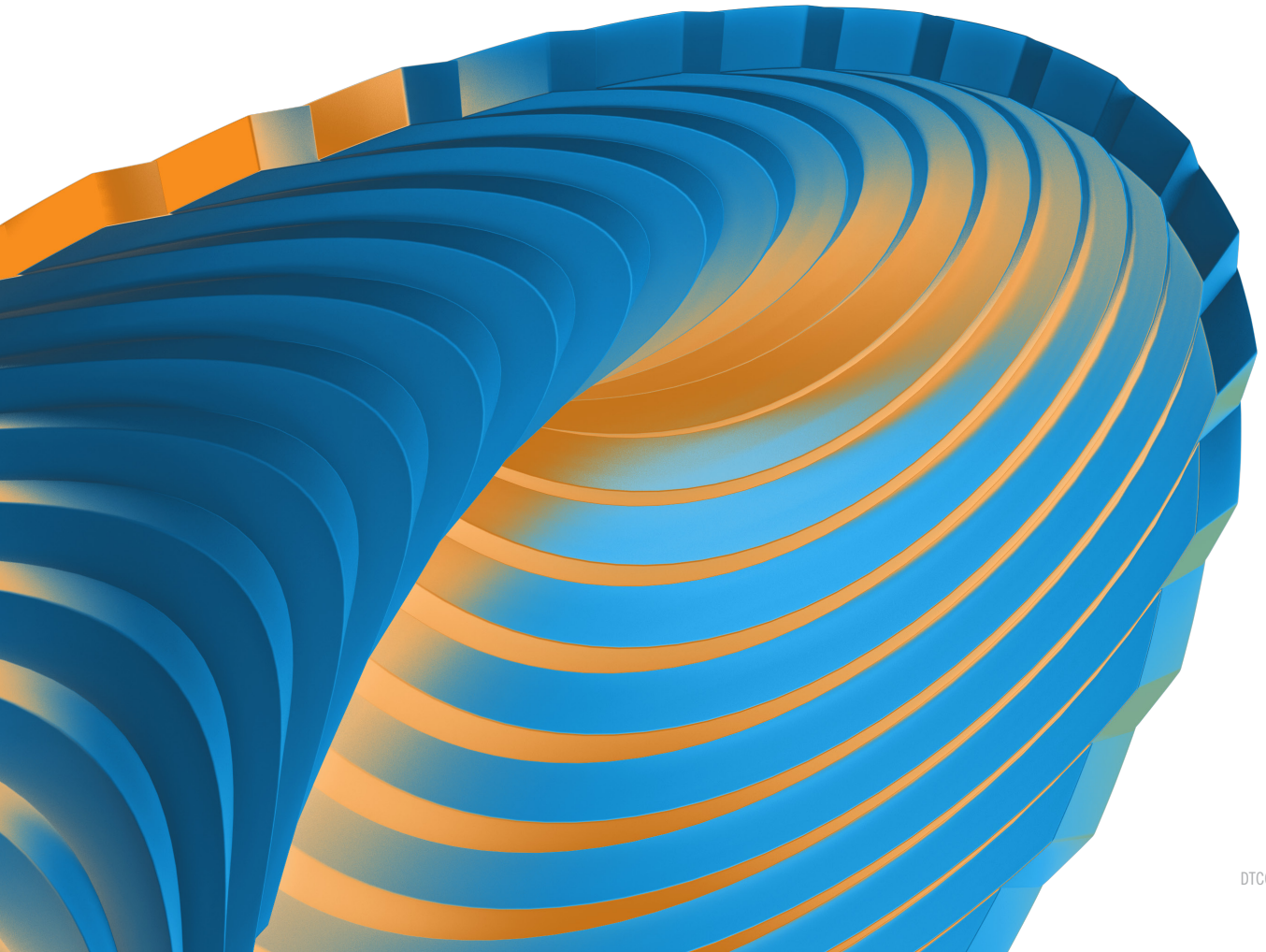


TABLE OF CONTENTS



INTRODUCTION

Today's technology has made it almost too easy to share data. Documents that once had to be signed in ink, mailed, or faxed can now be digitally signed, validated and sent with just a few simple keystrokes.

The digital transformation in the financial industry has brought powerful capabilities and efficiencies, but with these new, streamlined data sharing and processing methods come the potential for numerous negative impacts for risk management and data security if proper procedures are not followed.

DTCC's processing environment, in our Wealth Management Services (WMS) business, has evolved from more than 20 years of fintech research, investment, innovation and development to provide a secure, interconnected and layered suite of products and services – including Insurance & Retirement Services (I&RS), Mutual Fund Services (MF) and Alternative Investment Products (AIP).

In this report, DTCC's I&RS business shares a perspective on some industry trends recently observed. I&RS also offers guidance on some best practices to protect all categories of insurance and retirement data from theft and unauthorized access, with the help of technology, responsible processes, proactive controls – and above all, heightened awareness.

THE EMERGENCE OF RISKY & INEFFICIENT DATA-SHARING BEHAVIORS

DTCC's I&RS business has worked closely with the industry to develop streamlined processing and compliance-driven solutions for carriers and their distribution partners – broker/dealers, banks, brokerage general agencies, independent broker/dealers and other firms – through a secure, centralized and automated infrastructure. DTCC's infrastructure enables insurance carriers and distributors to securely exchange information at various points throughout the annuity and life insurance processing lifecycle.

I&RS has been alerted by clients and vendors to an alarming trend in the past year, especially with everyone dispersed and working remotely. I&RS has observed that – perhaps in the interests of short-term productivity – many firms have taken various cybersecurity shortcuts and increasingly started sharing data through workarounds such as sharing logins and passwords and sending unencrypted data in emails. Firms are also uploading data to external file share services and engaging in "screen-scraping," which is the act of copying information that shows on a digital display. While these data-sharing methods can be helpful, these methods are not centralized nor are they secured, and they can potentially allow sensitive and private data to fall into the hands of cybercriminals.

This data is not validated by the 'owner' of the data, which is typically the insurance carrier. These actions leave an organization vulnerable to data breaches, reputational risk and misinformation going to the end investor and producer.

EXAMPLES OF RISKY & INEFFICIENT DATA-SHARING BEHAVIORS

- Not encrypting data before sending
- Sending data through an unsecure email account
- Uploading data to external file sharing services
- Screen-scraping data
- Sending data while on an open, unsecured WIFI network
- Providing unauthorized system access with shared logins

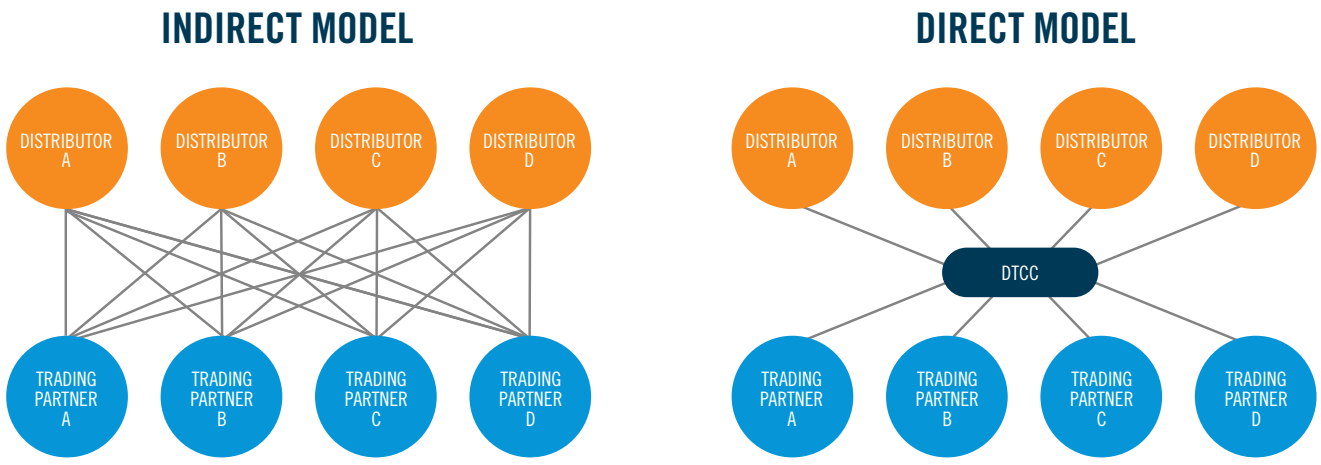
Another larger, concerning trend noted by I&RS is that firms have begun to revert to inefficient, indirect data processing models. This practice not only thwarts the industry's hard-fought progress to streamline and standardize data over the past 20+ years, but it also contravenes the very security protocols set by firms' Information Technology (IT) and Compliance teams, ostensibly putting their entire organizations' data at risk.

A SHIFT IN DATA EXCHANGE MODELS

The traditional, direct data exchange model including DTCC clients – banks and broker/dealers – is a centralized, automated processing solution addressing the needs of both insurance carriers and distributors. DTCC's role in the direct model was originally conceived as one of automation and connectivity between carriers and distributors; that role has now evolved significantly to being a "gatekeeper" of data security, redundancy, and standardization.

By contrast, the non-traditional, indirect sales channels – independent market organizations (IMO), brokerage general agents (BGA), registered investment advisors (RIA), etc. are generally more reliant on third-party service providers/vendors for services such as data aggregation, policy service and maintenance platforms. The indirect data exchange models were common back in the 1990s with complex data exchanging methods – proprietary data lines and feeds, overnighting disks on data, spreadsheets, etc.– that varied widely between organizations. Typically, it is very expensive to support business this way and creates multiple barriers to implementation and adoption.

Today, the non-traditional data exchange models are mostly new, third-party technology platforms. There are many more of them now than existed in the 1990s, and many are also unfamiliar with our industry's solutions to centralize and standardize data exchange. However, the current trend is that sales from the non-traditional distribution channels are seeing growth: according to Insured Retirement Institute's (IRI) Retirement Fact Book 2020 traditional, direct sales channel dropped in usage from 60.4% to 56.4% while non-traditional, indirect distribution channels rose from 15.2% to 23.2%[1].



This shift puts pressure on insurance carriers to support the data needs of many different service providers and vendors, leading to the complications, increased costs and inefficiencies as described earlier.

1 Beacon Research; Morningstar Inc. Annuity Total Sales Percentages by Distribution Channel

Recently, I&RS has observed a trend of clients moving from the security of direct data exchange models to the potentially riskier indirect models. I&RS has noticed that the change in model usage for many firms was influenced by some clients' own sales teams, including some of the following scenarios:

- **Carrier sales teams are investing their own technology budgets to initiate one-off/proprietary data feeds,** irrespective of the increased cost and additional maintenance requirements added to existing operations and technology groups, which is likely to negatively impact their data integrity – including the overall completeness, accuracy, and consistency of their data.
- **Clients are working with vendors to manage their implementations, but these vendors are also bypassing the direct model and instead interfacing directly with the insurance carriers to get their data.** This has the effect of creating a tremendous burden for the Carriers with complex implementations, with lack of standardized formats, lack of efficiency and added expenses to maintain – reverting to the "spaghetti" or proprietary model of data exchange seen 20+ years ago.
- **Many carriers are shifting focus and looking to new and non-traditional distribution channels.** As a result of this shift in focus, vendors new to the insurance space that have different technology capabilities are influencing how data is exchanged. This can impact security, data integrity and accuracy, but are more about low cost and rapid acquisition for vendors. In the long term, this may not be the best decision. For example, carriers are aware that some vendors are obtaining login credentials from legitimate customers. Then, they use that access to screen-scrape and bombard carrier platforms with thousands of website inquiries, resulting in websites crashing, unpredictable latency and ultimately, disruption of business.

The danger with Carriers not knowing that their data is being used by their trading partners' technology platforms is that it may result in a data breach or cyberattack, which could easily happen to any third-party financial platform lacking its own and/or organizational security protection. Following secure, standardized industry data exchange processes, such as those offered through DTCC, can greatly help mitigate these risks.

DATA SECURITY: THE COSTS AND CONSEQUENCES OF BREACHES & CYBERATTACKS

The financial industry – banking, insurance, investment companies, etc. – is a prime target for cybercriminals looking for financial gain and valuable data. Vulnerabilities have become even more notable since many companies were forced to quickly shift to remote working and cloud-based technologies last year due to the Covid-19 pandemic, with little time to fully plan out and test security efforts. In fact, during the Covid-19 pandemic from February to April 2020, there was a 238% increase in cyberattacks against financial services firms[2].

A survey conducted in 2021 by the Financial Services Information Sharing and Analysis Center (FS-ISAC) found that financial institutions had a substantial rise in cyberattacks like phishing – that is, stealing sensitive data or installing malware, usually with fraudulent emails that appear to be from a trustworthy source – as well as suspicious scanning and malicious activity against web pages for work-from-home (WFH) staff to access their firm's network during the Covid-19 pandemic[3]. Of the financial institutions surveyed by FS-ISAC, payment firms, insurance companies and credit unions have seen the largest increase in attacks.

The consequences of a data breach or cyberattack for a financial institution are serious and typically end up costing more to resolve – financially as well as to a firm's reputation and business intelligence – than ever would have been to proactively prevent.

According to **Verizon's 2021 Data Breach Investigation Report,** 44% of the breaches in the financial and insurance vertical were caused internally. Most were accidental, such as sending sensitive emails to the wrong people. However, this simple mistake alone represents a staggering 55% of all error-based breaches (and 13% of all breaches for the year).

- **Financial Consequences** – IBM Security's *Cost of a Data Breach Report* for 2021 found that the average total cost of a data breach was $4.24 million worldwide and around $8 million in the US, a 10% increase from the previous year[4]. For regulated industries, the average cost of a data breach is even more, with financial services, for instance, rising to $5.72 million. Organizations with high levels of compliance failures saw an average difference of $2.3 million more in breach costs when compared to organizations with low levels of compliance failures. Additionally, IBM Security found that the average cost increased by $1.07 million in breaches where remote work was a factor in causing the breach. At organizations that have more than half of their employees working remotely during the Covid-19 pandemic, IBM Security found that it's taken an average of 316 days to identify and contain a data breach. The research in the report showed that faster incident response times of 200 days or less correlated with cost savings of nearly 30%.

  There are several components that make up the "cost" of a data breach or cyberattack[5]. Short-term, direct expenses include engaging with forensic experts, immediate hardware or software purchases, contracted companies to assist in dissemination of information and a training hotline support to answer questions can all be common for during a data breach. Short-term, indirect costs of a data breach can include decreased company stock value, HR management aspects like individuals being let go, increased recruitment costs and training as well as employees and executives dropping day-to-day work to help mitigate the effects of the breach.

2 Experian 2021 Data Breach Response guide
3 BIS – Covid-19 and Cyber Risk in the Financial Sector
4 IBM 2021 Cost of a Data Breach Report
5 Sprinklr – How to Calculate the Cost of a Data Breach

The long-term direct costs of a data breach can consist of reimbursement of any fraudulent charges, providing free credit monitoring subscriptions, defending against lawsuits for negligence, failure to protect data, or violations of federal laws, paying compliance fines, funding internal investigations, or cooperating with third-party audits. There are also long-term indirect aspects like loss of customers, decreased future revenue, public relations (PR) and media crisis management, increased cyber insurance premiums, a damaged reputation and loss of business intelligence.

Overall, financially speaking, data breaches and cyberattacks are detrimental throughout an organization, especially an organization's bottom line. In the 2021 report, *Cyberwarfare in the C-Suite* by CyberSecurity Ventures, cybercrime is estimated to cost businesses $10.5 trillion annually worldwide by 2025, up from $3 trillion in 2015[6].

- **Reputation Consequences** – A damaged reputation is a long-term, indirect cost of a data breach or cyberattack. Executives, public relations (PR), relationship managers and more play a huge role in guiding the conversation around a data breach to preserve the organization's reputation while assuring current and potential customers that significant measures are being taken to prevent another cybersecurity event. Ultimately, data beaches and cyberattacks highlight a company's ability or lack thereof to respond to security situations and communicate throughout that process.
- **Business Intelligence Consequences** – During data breaches and cyberattacks, the security of many types of records can become compromised. Out of the breaches within the IBM Security's *Cost of a Data Breach Report* for 2021, customer PII (44%), anonymized customer data (28%), intellectual property (27%), employee PII (26%) and other sensitive data (12%) were the different compromised data categories[7]. Customer data-related categories are the most common in size and thought, however, another sizable category that isn't always thought about is intellectual property. Intellectual property infringement due to a data breach or cyberattack is a huge problem for a company's business intelligence strategies.

CONSEQUENCES OF DATA BREACHES & CYBERATTACKS

6 CyberSecurity Ventures - Cyberwarfare 2021 Report
7 IBM 2021 Cost of a Data Breach Report

DTCC'S INSURANCE & RETIREMENT SERVICES (I&RS) BEST PRACTICES FOR SHARING & PROCESSING DATA

With more financial institutions becoming aware of the dangers of data breaches and cyberattacks, many are looking to proactively evolve their data sharing and processing methods towards best practices. Below are some of the recommended best practices for clients from DTCC's I&RS business when sharing and processing insurance and retirement data:

1. **Don't participate in "work-around" data sharing practices:** Behaviors such as sharing logins, screen-scraping, copying and pasting, or sending data through an unsecured method put an organization at significant risk. Adhering to data exchange standard practices, such as those supported by DTCC, are a much safer and secure method of exchanging sensitive and private data.
2. **Have a secure, centralized location to store data:** A secure, centralized location to store data can be a cloud-based or can be an on-premise exchange platform such as **DTCC's Insurance Information Exchange (IIEX).**
3. **Avoid non-traditional data exchange models that don't meet security protocols:** Using a non-traditional model is typically inefficient, involves significant barriers for implementation, difficult to standardize data, is time consuming and lacks the centralization and automation that traditional models, like services at DTCC, can provide. When considering third-party vendors, make sure IT and Compliance are involved in the selection process, especially the security aspects, to avoid unnecessary risk.
4. **Use advanced authentication for accessing data when possible:** Decrease risk with advanced authentication methods like permissioned users, multi-factor authentication, authentication tokens or open banking API connections. DTCC offers and supports many data security authentication methods and encourages financial organizations to utilize these authentication methods to create the fastest, most secure, and most reliable connections in the industry.
5. **Protect data in cloud environments using encrypted data:** Any time data is being sent to a cloud platform such as Microsoft Azure, Oracle, Salesforce, Amazon Web Services (AWS), Google Cloud, be sure to encrypt it. Even if data is being sent in an email, it is going through the cloud and must be encrypted.
6. **Use secured networks when exchanging data:** Never share data while on a public or non-secured wireless internet network. Using secured tools like virtual private networks (VPN) or virtual desktop infrastructure (VDI) are the best methods to use when sharing data.
7. **Know the source of the data:** Don't download data from unknown sources like non-secured websites, file sharing sites or unfamiliar email addresses. Processing data through reliable entities like DTCC ensures that organizations are sending and receiving from trusted sources.
8. **Have standardized methods of sharing data:** Sharing data through the same mediums and with standardized fields, formatting and layouts helps keep data clean and organized. DTCC's I&RS has helped shape the industry by creating, implementing and enforcing adherence to data standards. The easier it is for employees to find and understand the data they are viewing, the more efficient an organization can be.
9. **Have a breach or cyberattack response plan:** Make sure your organization has breach and cyberattack response plans and a team who will be managing the crisis. Customers are more forgiving to organizations who promptly notify and handle a breach or cyberattack.
10. **Increase transparency and monitoring of data:** Financial organizations should be monitoring data in real-time, frequently testing data storage systems and conducting audits annually. All departments have a role to play in monitoring data and should be on the same page about data policies.

HOW DTCC SUPPORTS SHARING & PROCESSING DATA IN THE FINANCIAL INDUSTRY

DTCC has been a trusted staple in the financial industry for decades. Owned and operated by the industry gives DTCC a unique perspective on supporting best practices for sharing and processing data. DTCC's Wealth Management Services has several tools that specifically support clients' data needs across Insurance and Retirement Services (I&RS), Mutual Fund Services (MF), and Alternative Investment Products (AIP).

INSURANCE & RETIREMENT SERVICES (I&RS)

Insurance Information Exchange (IIEX): a platform for the exchange of policy, producer, and product data, provides clients with an easy, flexible, and secure data hub to support the sourcing and consumption of data.

BENEFITS

- Centralized data hub provides a standardized alternative to the need for sending large, redundant batch files
- Users can access easily consumable, purpose-driven and in force policy data files
- Additional phases will expand on the data offering across policy, producer and product details and will expand the data sourcing and delivery capabilities using new technologies
- Offers a solution for all insurance product types - annuities, life insurance and insurance-based retirement plans
- Stay compliant, meeting industry data standards through reactive regulatory changes
- Flexible, secure platform with API capabilities

LEARN MORE

MUTUAL FUND SERVICES (MF)

MF Info Xchange: facilitates and centralizes the delivery and receipt of time-critical mutual fund, bank collective fund and other pooled investment product notifications to reduce risk throughout the communication process.

BENEFITS

- Comprehensive portal supporting many types of notifications.
- Eliminates lengthy and complex notifications with pre-defined and standardized set of data elements.
- Audit Trail ability to view updates to notifications as well as other client activity performed within the portal.
- Event calendar enables users to view date-critical events, track historical event details, and remind receivers of upcoming events, all in one place.
- Consolidated Schedules view allows clients to provide monthly, quarterly, and annual Dividend/Capital Gain and Interval/Tender Fund Transaction schedules and helps manage these events.
- Seamless integration with MF Profile Security (DTCC's centralized data source of comprehensive fund prospectus and operational rules), automates the extraction of fund data and minimizes the risks associated with manual entries.
- Ability for notification receivers to designate email recipients by Event Type.
- Two-way communication between funds and intermediaries.

LEARN MORE

ALTERNATIVE INVESTMENT PRODUCTS (AIP)

MF Alternative Investment Products (AIP): is a standardized, trading and reporting platform that links the alternative investments industry to securely and efficiently exchange data and money.

BENEFITS

- Decreased cycle time to execute transactions
- Increased transparency into the status of transactions
- Decreased reliance on paper documents, faxes, emails and phone calls
- Reduced manual processing errors and risk
- Increased security and resiliency
- Improved compliance by leveraging AIP's designation as a good control location

LEARN MORE

GLOSSARY

- **Authentication Token** – aids in proving the user's identity and authenticating that user for the use of a service
- **Cyberattack** – a virtual attack targeting a company's use of cyberspace for the purpose of disrupting, disabling, destroying or maliciously controlling a computing environment/infrastructure
- **Cybercrime** – either a crime involving computing against a digital target or a crime in which a computing system is used to commit criminal offenses
- **Cybercriminal** – an individual who commits cybercrimes, where they make use of the computer either as a tool, as a target or as both
- **Cyber Insurance** – a form of insurance for businesses and individuals against internet-based risks
- **Data Breach** – is any unauthorized access and retrieval of sensitive information by an individual, group, or software system.
- **Data Integrity** – the overall completeness, accuracy, and consistency of data
- **Encrypted Data** – process of using an algorithm to transform plain text into cypher text in order to ensure that sensitive data remains unreadable to unauthorized users
- **Malicious Software (Malware)** – is any software that brings harm to a computer system
- **Multi-factor Authentication (MFA)** – is a security mechanism in which individuals are authenticated through more than one required security and validation procedure
- **Personally Identifiable Information (PII)** – information that, when used alone or with other relevant data, can identify an individual
- **Phishing** – stealing sensitive data or installing malware with fraudulent emails that appear to be from a trustworthy source
- **Secured Network** – is a wireless network that encrypts and secures all communications by default
- **Screen-Scraping** – the process of collecting screen display data from one application and translating it so that another application can display it
- **Unencrypted Data** – refers to data or information that is stored unprotected, without any encryption
- **Virtual Desktop Infrastructure (VDI)** – is a virtualization technique enabling access to a virtualized desktop, which is hosted on a remote service over the Internet
- **Virtual Private Network (VPN)** – is a private network connection that is built over a public network infrastructure such as the internet

WHITE PAPER REFERENCES

- **2021 Report: Cyberwarfare in the C-Suite**
  www.cybersecurityventures.com
- **Covid-19 and Cyber Risk in the Financial Sector**
  www.bis.org
- **Experian 2021 Data Breach Response Guide**
  www.experian.com
- **How to Calculate the Cost of a Data Breach**
  blog.sprinklr.com
- **IBM Cost of a Data Breach Report 2021**
  www.IBM.com
- **IRI Retirement Fact Book 2020**
  www.myirionline.org
- **Verizon 2021 Data Breach Investigations Report**
  www.verizon.com

GLOSSARY REFERENCES

- **Investopedia**
  www.investopedia.com
- **National Institute of Standards and Technology, U.S. Department of Commerce**
  www.nist.gov
- **Techopedia**
  www.techopedia.com

DTCC'S HELPFUL LINKS

- **Alternative Investment Products**
- **Client Cybersecurity Program**
- **Cyber Threats and Data Recovery for FMIS White Paper**
- **Four Strategies for Patching Up Rushed Remote-Working Infrastructures**
- **Insurance Information Exchange**
- **Mutual Fund Info Xchange**
- **Wealth Management Services**

For more information on our products and services, visit DTCC.com

For information on careers at DTCC, visit careers.dtcc.com

FOLLOW US ON

DTCC

ADVANCING FINANCIAL MARKETS. TOGETHER.™

 27313_LC112021 DTCC Public (White)