

# Mitigate Risk and Optimize Experience

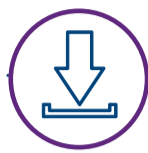
Modernize. Transform. Protect.



The cybersecurity landscape is increasingly volatile. One example is the recent cybersecurity breach involving the MOVEit Transfer Application, used by organizations worldwide.

The “zero-day” vulnerability in the MOVEit Transfer Application allowed data to be downloaded by an unauthorized third party.

## What Happened



Personal information was downloaded and included: first and last name; date of birth (DOB); and Social Security number (SSN).



Also, the names of former or current employers, spouses or domestic partners, and children.



The information that was taken involves anyone who was receiving an ongoing monthly benefit payment as of this spring.

## The Impact



The MOVEit breach could be the **most devastating exploitation of a zero-day vulnerability ever, and the effects continue to ripple across the globe.**

The widely used file-transfer program’s vulnerability has led to new victims coming forward weekly.<sup>1</sup>



However, only a minority of victims have so far reported the number of individuals impacted. If the same average number of individuals are confirmed to have been impacted in each of the remaining known incidents, **the cost will be \$38,013,902,301.** Note that this number is based on known victims, and not all victims are currently known.<sup>2</sup>



The MOVEit exploitation **appears to have affected at least 122 organizations and exposed the data of roughly 15 million people.** These numbers are based on posts from CL0P, the Russian ransomware group that has claimed responsibility for the attacks.<sup>1</sup>



... at least **seven of the known MOVEit victims are U.S. universities, and 16 are U.S. public sector organizations.**<sup>3</sup>



The MOVEit hack spawned around **600 breaches but isn't done yet.**<sup>1</sup>



This includes the **U.S. Department of Health and Human Services (HHS), according to Bloomberg, which reported ... that officials notified Congress of an incident involving the exposure of more than 100,000 individuals.**<sup>2</sup>



Based on the numbers of individuals confirmed to have been impacted, that puts the **cost of the MOVEit incident at \$6,551,884,185.**<sup>2</sup>

## How to Mitigate the Impact



Ensure accurate payments to retirees and beneficiaries.



Enable ability to transfer data to and from in a secure, encrypted format.



Properly confirm member deaths.



Prevent payments to bad actors or fraudsters.



Confirm information on inactive members who may soon be eligible for benefits.

## The Solution:



**Quality data** not just from the credit bureaus. Alternative data sourcing is key.



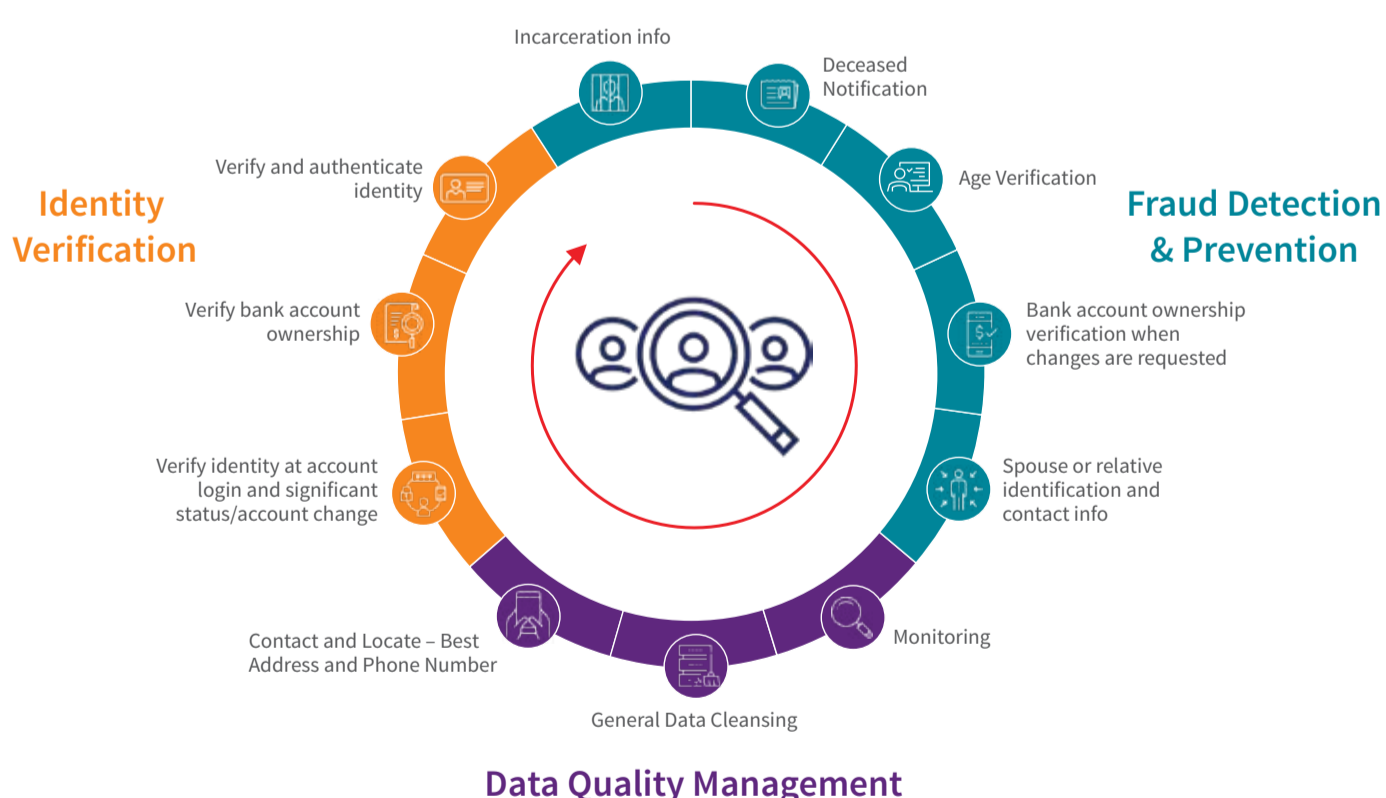
**Encryption and tokenization** for secure transfers of data back and forth.



**Trusted data stewardship** to protect privacy and ensure cybersecurity is critical.

## One Seamless and Secure Solution

Comprehensive identity verification, fraud prevention and data quality management



### Comprehensive Identity Management

- Data Hygiene/ Cleansing**
  - Deceased— not just Master File
  - Best Name, Address, DOB, SSN
  - Relatives and Associates
- Data Enrichment**
  - Mailing Contacts / Address Verification
  - Bank Account Ownership Verification
  - Derogatory Financial Information (Collections/Liens/Bankruptcy)
- Data Anonymizing (Single Unique Identifier- Non-Personal Identifiable Information (PII))**
- Identity Verification**

### Seamless Delivery

- People and Business Batch Solutions**
  - Frequency on demand (one-time, quarterly, daily, hourly)
  - Custom batch to meet specific needs
  - Secure File Transfer Protocol (SFTP) process with multiple file layout options
- Population Monitoring on Data Changes**
  - Dedicated LexisNexis Risk Solutions batch consultant will manage the entire process and verify results and answers output questions
- Summary Report & Result Analysis**
- Predictive Risk Analysis after Implementation Batch**
- LexisNexis® AmplifyID™ Identity Risk Navigator** can monitor your population on an ongoing basis

### Privacy and Trust Assurance

- 50 years** managing sensitive data
- Comprehensive Risk Framework** that incorporates standards for information security (**ISO 270001/2**) **code of practice and privacy (AICPA/CICA)** as well as other proprietary credentialing and security criteria.
- Proven Information Security Program** designed to protect the **security, confidentiality and integrity of personal information** collected from about consumers made available through any product or service.
- The Forrester Wave™ 2022 Leader in Identity Verification**
- Best Cybersecurity Provider 2022** The Waters Rankings



**LexisNexis®**  
RISK SOLUTIONS

For more information, scan QR code or call 1-800-869-0751



Sources:  
1 <https://www.reuters.com/moveit/moveit-hack-spawned-around-600-breaches-isnt-done-yet-cyber-analysts-2023-08-08/>  
2 <https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/>  
3 <https://techcrunch.com/2023/06/29/millions-affected-moveit-mass-hacks/>

The LexisNexis Emailage, FlexID, Bank Account Owner Verification, Batch, AmplifyID Identity Risk Navigator and ThreatMetrix for Government services referred to herein are not provided by “consumer reporting agencies,” as that term is defined in the Fair Credit Reporting Act (15 U.S.C. § 1681, et seq.) (“FCRA”) and do not constitute “consumer reports,” as that term is defined in the FCRA. Accordingly, the LexisNexis Emailage, FlexID, Bank Account Owner Verification, Batch, and ThreatMetrix for Government services may not be used in whole or in part as a factor in determining eligibility for credit, insurance, employment or another purpose in connection with which a consumer report may be used under the FCRA. Due to the nature of the origin of public record information, the public records and commercially available data sources used in reports may contain errors. Source data is sometimes reported or entered inaccurately, processed poorly or incorrectly, and is generally not free from defect. This product or service aggregates and reports data, as provided by the public records and commercially available data sources, and is not the source of the data, nor is it a comprehensive compilation of the data. Before relying on any data, it should be independently verified. LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc. Emailage is a registered trademark of Emailage Corp. ThreatMetrix is a registered trademark of ThreatMetrix, Inc. AmplifyID is a trademark of LexisNexis Risk Solutions Inc. © 2023 LexisNexis Risk Solutions. NXR16167-00-0823-EN-US