UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

IN RE: MOVEIT CUSTOMER DATA SECURITY BREACH LITIGATION This Document Relates To: ALL CASES	MDL No. 1:23-md-03083-ADB-PGL Common Complaint

PLAINTIFFS' OMNIBUS SET OF ADDITIONAL PLEADING FACTS

TABLE OF CONTENTS

Page

PLAINTIFFS' OMNIBUS SET OF ADDITIONAL PLEADING FACTS

All Plaintiffs in this proceeding allege as follows:

1. This case concerns a massive data breach (the "Data Breach") in which culpability for the breach is shared by the software developer, Defendant Progress Software Corporation ("Progress"), as well as the entities that used Progress's software.

2. At the heart of the Data Breach is Progress's file-transfer software called MOVEit, which had a known defect and vulnerability that was exploited by threat actors in and around May 2023.

3. The vulnerability, which had been tested by the threat actors since 2021, was a software code defect that allowed the threat actors to gather information on millions of individuals in a highly automated way.

4. As a result of the Data Breach, sensitive personal information belonging to millions of individuals, including Plaintiffs and Class Members, can now be found on the dark web, placing those individuals at risk of fraud and identity theft now and well into the future.

PARTIES

5. Defendant **Progress Software Corporation** is a public corporation organized under the laws of the State of Delaware with its principal place of business located at 15 Wayside Road, Suite 4, Burlington, Massachusetts 01803.

6. Progress produces software for creating and deploying business applications. Founded in 1981 in Burlington, Massachusetts, it has offices in 16 countries, thousands of employees, and revenues of over $500 million.[1]

[1] 10-K, Progress Software Corporation (Nov. 30, 2021, filed Jan. 27, 2022), https://investors.progress.com/sec-filings/sec-filing/10-k/0000876167-22-000038.

7. Originally called Data Language Corporation, the company changed its name to Progress Software in 1987. In 2016, Progress Software re-branded to "Progress" in an effort to "shed any doubts it was not living up to its name."[2]

8. Progress has seen rapid expansion over the past two decades, acquiring eXcelon Corporation for approximately $24 million in 2002, DataDirect Technologies in 2003 for $88 million, Persistence Software in 2004 for $16 million, and at least a dozen other companies for well over $200 million since then.[3]

9. Progress's insatiable appetite for growth also resulted in its acquisition of Ipswitch, Inc., an IT management vendor known for its MOVEit managed file transfer platform, in 2019 for $225 million.[4]

10. **Other Defendants** have also been named as part of the above-captioned multidistrict litigation, and claims against these Defendants are addressed in individual complaints which have been transferred to this Court for coordinated or consolidated pretrial treatment.

[2] Justine Hofherr, *After 35 years, Progress Software introduces a new name and vision*, Bulletin Bostin (Nov. 8, 2016), https://www.builtinboston.com/articles/after-35-years-progress-software-introduces-new-name-and-vision.

[3] Andrew Phelan, *Trinity boys sell college firm for $162m*, Irish Independent (Jun. 26, 2008), https://www.independent.ie/regionals/herald/trinity-boys-sell-college-firm-for-162m/27876930.html; Darryl K. Taft, *Progress Software Acquires Iona*, eWeek (June 25, 2008), https://www.eweek.com/development/progress-software-acquires-iona/; Scarlet Pruitt, *Progress buys XML toolmaker eXcelon*, Computerworld (Oct. 21, 2022), https://www.computerworld.com/article/1336237/progress-buys-xml-tool-maker-excelon.html; *Progress Software acquires algorithmic technology vendor Apama*, Finextra (Apr. 7, 2005), https://www.finextra.com/newsarticle/13477/progress-software-acquires-algorithmic-technology-vendor-apama; Yogesh Gupta, *Progress to Acquire NoSQL Database Pioneer, MarkLogic*, Progress Blogs (Jan. 3, 2023), https://www.progress.com/blogs/progress-to-acquire-nosql-database-pioneer-marklogic.

[4] Larry Dignan, *Progress acquires Ipswitch for $225 million, tops first quarter targets*, ZDNet (Mar. 28, 2019), https://www.zdnet.com/article/progress-acquires-ipswitch-for-225-million-tops-first-quarter-targets/; *Progress Completes Acquisition of Ipswitch, Inc.*, Progress: Press Release (May 1, 2019), https://investors.progress.com/news-releases/news-release-details/progress-completes-acquisition-ipswitch-inc#.

FACTUAL ALLEGATIONS

I. The MOVEit Software.

A. MOVEit software and its use by various Defendants.

11. MOVEit is a file transfer program used by a wide range of organizations in the public and private sector to move highly sensitive consumer data.

12. Financial services companies, government agencies, pension funds, hospitals, universities, banks, health systems, energy and technology companies, and a wide variety of other institutions use the MOVEit product.

13. MOVEit is offered in both on-premises—MOVEit Transfer—and cloud-based—MOVEit Cloud—versions.

1. MOVEit Transfer.

14. Standard Networks, Inc. first developed and released the MOVEit family of software in February 2002 to allow customers to securely transfer files over the Internet.[5] Standard Networks, Inc. was acquired by Ipswitch, Inc.,[6] which was then acquired by Progress in 2019.[7]

15. MOVEit Transfer is software that is licensed to customers on a subscription basis and installed by customers on their own servers.[8]

---

[5] *Standard Networks releases secure transfer client*, WTN News (Mar. 24, 2004), http://wtnnews.com/articles/700/ [https://web.archive.org/web/20110807192045/http://wtnnews.com/articles/700/].

[6] *Standard Networks acquired by Ipswitch*, Milwaukee Bus. J. (Feb. 19, 2008), https://www.bizjournals.com/milwaukee/stories/2008/02/18/daily8.html.

[7] Dignan, *supra* note 4.

[8] *Modules: MOVEit Transfer*, Progress: MOVEit, https://www.progress.com/moveit/moveit-transfer (last visited Apr. 26, 2024).

16. MOVEit Transfer is an "on-premises solution" that allows users to have complete control over business-critical file transfers by consolidating them in one system on their own premises.[9]

17. One of MOVEit Transfer's selling points was its use of SSL/TLS to securely transfer files as well as AES for encrypted storage of files (both described in further detail below), thus ensuring that files can only be read if the user has the appropriate encryption keys, even if the files are stolen.[10]

18. SSL, standing for "Secure Sockets Layer," is an encryption protocol developed in 1995 to communicate securely and privately over the Internet. SSL is the predecessor to TLS, developed in 1999 and standing for Transport Layer Security, which is the standard today. TLS uses a combination of public and private keys to encrypt and decrypt data that is passed over a network, such as the Internet. Use of TLS by a website is denoted by "https," as opposed to "http," in the website address.[11] TLS is virtually unbreakable with existing technology.[12]

19. AES, standing for Advanced Encryption Standard, is the standard for encryption of electronic data adopted by the United States government since 2001. AES uses a private key to

[9] MOVEit Transfer, https://www.ipswitch.com/moveit-transfer (last visited Apr. 26, 2024).

[10] *Id*.

[11] *What is SSL? | SSL definition*, Cloudflare, https://www.cloudflare.com/learning/ssl/what-is-ssl/ (last visited Apr. 26, 2024).

[12] Dionisie Gitlan, *Cracking SSL Encryption is Out of Human Reach*, SSL Dragon (Apr. 15, 2024), https://www.ssldragon.com/blog/cracking-ssl/.

both encrypt and decrypt data.[13] AES is widely adopted and used around the world by governments, businesses, and software.[14] AES is virtually unbreakable with existing technology.[15]

20. Pursuant to the MOVEit Transfer end user license agreement, Progress provides "bug fixes, patches, upgrades, enhancements, new releases [and] technical support" to customers.[16]

21. MOVEit Transfer's customers are primarily businesses, organizations, and governmental entities. Customers install MOVEit Transfer on their servers, and then users—such as the customer's employees—access the software through a MOVEit Transfer software client installed on a computer or phone or a website accessible over the Internet that connects to the customer's MOVEit Transfer server.[17]

22. Below are examples of the MOVEit Transfer user interface[18]:

[13] Nat'l Inst. of Standards. & Tech., *Advanced Encryption Standard (AES)*, Fed. Info. Processing Standards Publ'n 197-upd1 (May 9, 2023), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf.

[14] Rahul Awati et al., *What is the Advanced Encryption Standard (AES)?*, TechTarget (Feb. 2004), https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard.

[15] Victor Kananda, *Why You Should Use AES 256 Encryption to Secure Your Data*, Progress: Blogs (Jun. 22, 2022), https://www.progress.com/blogs/use-aes-256-encryption-secure-data.

[16] *MOVEit and WS_FTP End User License Agreement*, Progress: Legal Info. (Nov. 2023), https://www.progress.com/legal/license-agreements/moveit-ws-ftp.

[17] *Introduction*, *MOVEit Transfer 2023.1 Adm'r Guide*, Progress: Prod. Documentation (Apr. 21, 2022), https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2023/page/Introduction.html; *Client Access*, *MOVEit Transfer 2023.1 Adm'r Guide*, Progress: Prod. Documentation (Apr. 6, 2022), https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2023/page/Client-Access.html.

[18] *Id.*

Figure 1

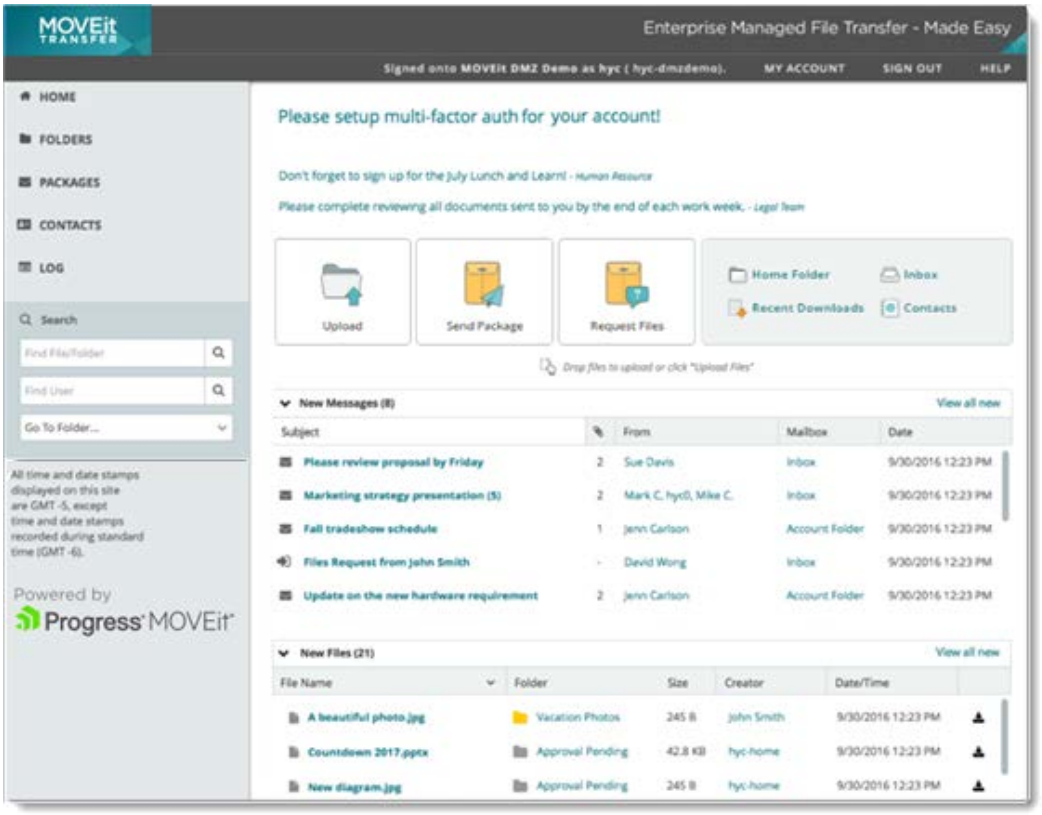
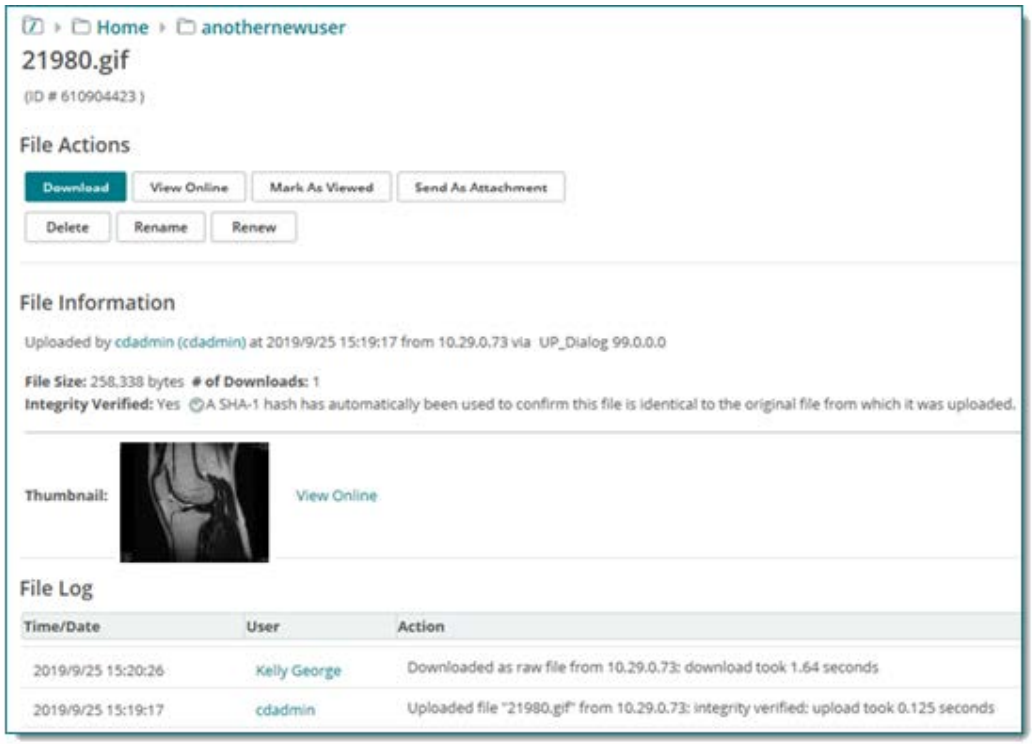

MOVEit TRANSFER
Enterprise Managed File Transfer - Made Easy
Signed onto MOVEit DMZ Demo as hyc (hyc-dmzdemo).
MY ACCOUNT
SIGN OUT
HELP
HOME
FOLDERS
PACKAGES
CONTACTS
LOG
Search
Go To Folder...
All time and date stamps displayed on this site are GMT -5, except time and date stamps recorded during standard time (GMT -6).
Powered by Progress MOVEit
Please setup multi-factor auth for your account!
Don't forget to sign up for the July Lunch and Learn! - Human Resource
Please complete reviewing all documents sent to you by the end of each work week. - Legal Team
Upload
Send Package
Request Files
Home Folder
Inbox
Recent Downloads
Contacts
Drop files to upload or click "Upload Files"
New Messages (8)
View all new
Subject
From
Mailbox
Date
Please review proposal by Friday
Sue Davis
Inbox
9/30/2016 12:23 PM
Marketing strategy presentation (5)
Mark C, hyc0, Mike C.
Inbox
9/30/2016 12:23 PM
Fall tradeshow schedule
Jenn Carlson
Account Folder
9/30/2016 12:23 PM
Files Request from John Smith
David Wong
Inbox
9/30/2016 12:23 PM
Update on the new hardware requirement
Jenn Carlson
Account Folder
9/30/2016 12:23 PM
New Files (21)
View all new
File Name
Folder
Size
Creator
Date/Time
A beautiful photo.jpg
Vacation Photos
245 B
John Smith
9/30/2016 12:23 PM
Countdown 2017.pptx
Approval Pending
42.8 KB
hyc-home
9/30/2016 12:23 PM
New diagram.jpg
Approval Pending
245 B
hyc-home
9/30/2016 12:23 PM

Figure 2



23. Users can also access MOVEit Transfer through a REST API, a programmatic means of interacting with the MOVEit Transfer server without using a graphical user interface such as a client or website.[19]

24. Because the MOVEit Transfer software is installed on customers' public-facing Internet servers, not Progress's servers, the software is accessible by accessing the customers' public website—for example, through *http://moveit.customer-domain-name.com*—not Progress's website.[20]

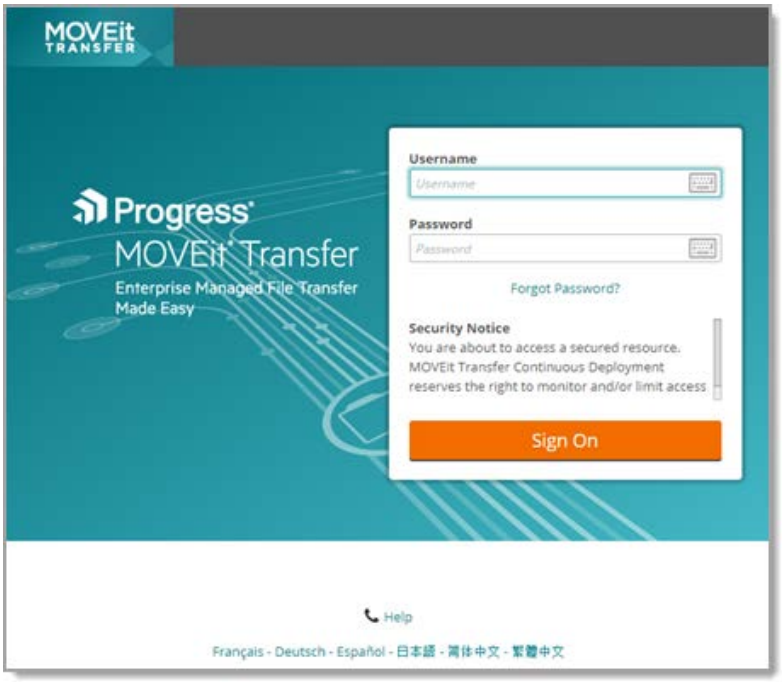
[19] *Id.*

[20] *Advanced Topics: Systems Internal – URL Crafting, MOVEit Transfer 2023.1 Adm'r Guide*, Progress: Prod. Documentation (Apr. 21, 2022), https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2023/page/System-Internals-URL-Crafting.html.

25. Authorized users must log into the MOVEit Transfer server with a username and password.[21]

26. Below is a default user login page that would be accessible from a MOVEit Transfer customer's public-facing website on the Internet[22]:

Figure 3



27. After authenticating, users can then transfer files to the MOVEit Transfer server by uploading or downloading files through the MOVEit Transfer client or web application.[23]

28. Progress claims MOVEit Transfer encrypts files both in transit and at rest so they cannot be viewed at any time without the appropriate encryption key.[24]

---

[21] *User Guide Welcome: Sign-on, MOVEit Transfer 2023.1 Adm'r Guide*, Progress: Prod. Documentation (Aug. 4, 2022), https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2023/page/Sign-On.html.

[22] *Advanced Topics: Systems Internal – URL Crafting*, *supra* note 20.

[23] *Introduction, MOVEit Transfer 2023.1 Adm'r Guide*, *supra* note 17.

[24] *Id.*

2. MOVEit Cloud.

29. Ipswitch developed MOVEit Cloud in 2012.[25]

30. MOVEit Cloud enables the consolidation of all file transfer activities into a cloud-based, online service using Microsoft Azure Cloud servers managed by Progress.[26]

31. While previous MOVEit products required Progress's software to be installed and run on the customers' servers, MOVEit Cloud operates on Progress's servers, thus removing the need for customers to maintain their own servers.[27]

32. Accordingly, customers that use MOVEit Cloud do not need to update and patch software installed on their own servers because MOVEit Cloud is maintained by Progress and runs only on Progress servers.[28]

3. How MOVEit is used.

33. MOVEit software is used by different entities in order to transfer sensitive information.

34. Progress boasts that MOVEit is the "leading secure Managed File Transfer (MFT) software used by thousands of organizations around the world to provide complete visibility and control over file transfer activities. Whether deployed as-a-Service, in the Cloud, or on premises, MOVEit enables your organization to meet compliance standards, easily ensure the reliability of

[25] Brandon Butler, *File transfer systems adapting to today's cloudy conditions*, NetworkWorld (Nov. 13, 2012), https://www.networkworld.com/article/666073/cloud-computing-file-transfer-systems-adapting-to-today-s-cloudy-conditions.html.

[26] MOVEit Cloud, https://www.ipswitch.com/moveit-cloud (last visited Apr. 26, 2024).

[27] *Id.*

[28] *Modules: MOVEit Cloud*, Progress: MOVEit, https://www.progress.com/moveit/moveit-cloud (last visited Apr. 26, 2024).

core business processes, and secure the transfer of sensitive data between partners, customers, users and systems."[29]

35. MOVEit helps information technology teams "at almost every federal civilian agency and military branch to securely transfer mission-critical information and assure the performance of their networked infrastructures and applications."[30]

36. Many businesses rely on third parties to provide useful software and code as elements of the supply chain for their own services or applications.

37. In this case, entities could either contract directly with Progress to use MOVEit software (either on-premises via MOVEit Transfer or online via MOVEit Cloud), or contract with a third-party which used MOVEit software. A variety of parties—such as direct users or vendors—thus used MOVEit software to effectuate file transfers. *See* Exhibit A (Updated Defendant Track Appendix A).

B. Progress warrants the security of its software.

38. Progress knows and intends that its customers use MOVEit software to transfer highly sensitive personally identifiable and protected health information ("Private Information").

39. Progress markets, advertises, and warrants MOVEit software as having industry-leading robust data security that complies with applicable data security laws and will keep Private Information from being compromised.

40. Regarding Progress's data security policies and practices, Progress states:

> Progress MOVEit helps your organization meet cybersecurity compliance standards such as PCI-DSS, HIPAA, GDPR, SOC2 and

[29] MOVEit, Managed File Transfer Software, Progress (formerly Ipswitch), https://www.ipswitch.com/moveit (last visited Apr. 26, 2024).

[30] IT Solutions, US Federal Government, Progress, https://www.ipswitch.com/industries/government-us-federal-government (last visited Apr. 26, 2024).

more. Provide a more secure environment for your most sensitive files, while supporting the reliability of core business processes.[31]

* * *

The security of our customers' environments is paramount. Progress has a comprehensive cybersecurity program in place which includes a zero-trust cybersecurity architecture approach, compliance audits and verifications, source-code scanning, external penetration tests, third-party deep-dive code assessments as well as ongoing coordination with some of the industry's top cybersecurity researchers.

When vulnerabilities are found, we work quickly to mitigate the risk, issue appropriate patches and communicate directly with our customers, so they can take immediate action to harden their environments against those vulnerabilities.[32]

* * *

Employee Security Awareness

All employees undergo a regimen of security training throughout the year. Content is selected by committee and features such topics as General Security awareness, email security, phishing awareness, HIPAA ePHI Training, GDPR training, and secure coding.

Security Architecture Planning

Company Security Architecture planning is an ongoing activity managed by Corporate Information Security and Product Information Security Staff. Throughout the course of a given year risks are identified and tracked, existing information Security solutions are monitored, and new Security Technologies are researched for possible implementation. Standard approaches to perimeter Network Security, cloud infrastructure security, web and application security, authentication, and database security are just some of the disciplines we focus on. Our engineers work together within products and across products to ensure best practices in security design are implemented and maintained.

[31] *MOVEit*, Progress, https://www.progress.com/moveit (last visited Apr. 26, 2024).

[32] *Security Center*, Progress, https://www.progress.com/security (last visited Apr. 26, 2024).

Security Defense

From corporate networks, to web applications, to cloud offerings, to employee computing environments, Progress employs a defense in depth strategy in the protection of our corporate assets and our customer environments. Network perimeter security, intrusion detection and prevention, anti-malware, anti-virus, server hardening, secure load balancing, secure authentication, encryption of data in transit, encryption of data at rest, stringent user access control, database security, security monitoring, and event management are just a few of the technologies involved in protecting our business and our customers.

* * *

Product Security

All software products at progress are developed a via the use of modern methodologies, techniques, technologies, and processes. Our software development life cycles employ Agile methodologies while including numerous waves of security planning and testing. These include security requirements planning, security design planning, code level security scanning, vulnerability scanning, and penetration testing.

Threat and Vulnerability Management

Ongoing threat and vulnerability management activities performed on all corporate assets and customer facing product environments. These activities include monitoring of key government and media outlets to stay apprised of emerging security issues, vulnerability scanning of internal and external systems, penetration testing of products and corporate environments.

Remediation Management

Progress subjects itself to a regular regimen of assessment activities to identify information security risks. Such activities may include self-initiated security assessments via a contracted 3rd party security firms, systems controls reviews by external industry authorities, or internal assessment activities using the expertise of existing staff. As such activities are conducted, any finding will be processed in a consistent manner that mitigates risk.

Security Incident Management

The Executive Security Committee at Progress has directed that an Incident Management function be operated that handles all

> corporate and customer related incident matters. In the case of an information security incident that threatens the availability, confidentiality, and integrity of information assets, information systems, and the networks that deliver the information, a response is conducted in a consistent manner. Appropriate leadership and technical resources are involved in any incident situation, in order to make key decisions and promptly restore any operations impacted. Exercises are performed on a recurring basis to ensure staff familiarity with procedures and identify any new lessons that should be incorporate into response plans.[33]

41. Regarding MOVEit Transfer's data security, Progress specifically states:

> **More Secure Managed File Transfer Software for the Enterprise**
>
> Leverage MOVEit Transfer's file encryption, security capabilities, tamper-evident logging, activity tracking and centralized access controls to help meet your operational requirements. Facilitate compliance with SLAs, internal governance requirements and regulations like PCI, HIPAA, CCPA/CPRA and GDPR.
>
> * * *
>
> **Transfer Sensitive Information More Securely**
>
> Help secure enterprise data in transit and at rest with advanced security features and encryption (FIPS 140-2 validated AES-256 cryptography). Better enforce user, system and file security policies while controlling the movement of sensitive files. Leverage user authentication, delivery confirmation, non-repudiation and hardened platform configurations.[34]
>
> * * *
>
> **Aid Secure End User Collaboration**
>
> When sensitive data is likely to be externally shared by end users, MOVEit's Ad Hoc, Secure Folder Sharing and MOVEit Client provide a more secure, convenient and easy-to-use alternative to unsafe email and content collaboration. This allows IT teams to strengthen data security, visibility and audit trails and compliance

[33] *Info. Sec. Program Whitepaper*, Progress: Legal Info., https://www.progress.com/security/information-security-program-whitepaper (last visited Apr. 26, 2024).

[34] *Modules: MOVEit Transfer*, *supra* note 8.

> with data protection regulations such as PCI, HIPAA, CCPA/CPRA and GDPR.
>
> * * *
>
> **Easily implement added security controls and establish an audit trail.**
>
> Because transfers are logged in a tamper-evident database, MOVEit Transfer helps facilitate compliance with SOC2, PCI-DSS, HIPAA, GDPR and other data privacy regulations. It provides pre-defined and customizable reports and logging of all data interactions, including files, events, people, policies and processes.
>
> * * *
>
> **Provide alternatives to risky transfer methods.**
>
> Improve the secure and compliant transfer of protected data by providing users with easy-to-use alternatives to risky transfer methods. Secure Folder Sharing provides a convenient, easy-to-use alternative to consumer-grade file sharing services. MOVEit Client helps provide access to secure transfers from Windows and MacOS desktops. MOVEit Ad-Hoc helps make secure file transfer easily accessible via email, either from Microsoft Outlook or a web browser. MOVEit Mobile enables access from iOS or Android devices.[35]

42. Progress "***guarantees*** the security of sensitive files both at-rest and in-transit."[36]

43. Progress, by marketing and advertising the MOVEit software as a solution for secure transfer and storage of files containing highly sensitive Private Information, knew or should have known that it was responsible for: keeping customers' files private; complying with industry standards related to data security and maintenance of its customers' files and the Private Information contained therein; ensuring the security of customers' files and the Private Information contained therein to protect them from unauthorized disclosure and exfiltration; and

[35] *Id.*

[36] Corporate Brochure, Progress (2023), https://d117h1jjiq768j.cloudfront.net/docs/default-source/default-document-library/progress-corporate-brochure-2023-rgb.pdf (emphasis added).

providing adequate notice to customers and individuals if their Private Information was disclosed without authorization.

C. The vulnerabilities in Progress's software.

1. SQL injection vulnerability.

44. MOVEit Transfer logs transfers in an SQL database that is also maintained by the customer on their network.[37]

45. SQL, developed in the 1970s and standing for Structured Query Language, is one of the most popular programming languages for interacting with relational databases, databases that store data in tables made up of rows and columns. Many of the most popular relational database providers and implementations use SQL, including MySQL and Oracle. SQL commands use common English words such as INSERT, UPDATE, DELETE, etc., which make the language intuitive and easy to learn. An SQL engine takes an SQL query or statement as input, parses it into executable code, and then executes that code to return any matching rows in the database. As long as the SQL statement inputted can be parsed as valid SQL, the database can execute it.[38] Because SQL is used only to access a database, it is used alongside other server-side programming languages that perform other functions of a server, such as validating user input or creating web pages. Other server-side programming languages also have built-in functions that can create SQL queries and send queries to an SQL engine.[39]

---

[37] *MOVEit Transfer High Availability (HA) Data Sheet*, Progress, https://www.ipswitch.com/resources/data-sheets/moveit-transfer-high-availability (last visited Apr. 26, 2024).

[38] *What is SQL (Structured Query Language)?*, Amazon Web Servs., https://aws.amazon.com/what-is/sql/ (last visited Apr. 26, 2024)..

[39] *See, e.g.*, *Create a SQL Server Database programmatically by using ADO.NET and Visual C# .NET*, Microsoft (May 7, 2022), https://learn.microsoft.com/en-us/troubleshoot/developer/visualstudio/csharp/language-compilers/create-sql-server-database-programmatically.

46. When a customer logs into or uses the MOVEit Transfer web application, they may input some information into form fields (*e.g.*, email, password, or other user-inputted information), which is then transmitted to the MOVEit Transfer server running on the customer's network to be interpreted and processed by the MOVEit Transfer software. Some user input is passed to the MOVEit Transfer SQL database as part of the query (*e.g.*, comparing credentials inputted by a user to credentials stored in the database, or searching a table for a certain record).[40]

47. The simplicity of SQL makes it both very useful and highly vulnerable to exploitation through SQL injection.[41]

48. SQL injection is described in the Common Weakness Enumeration database as follows:

> Without sufficient removal or quoting of SQL syntax in user-controllable inputs, the generated SQL query can cause those inputs to be interpreted as SQL instead of ordinary user data. This can be used to alter query logic to bypass security checks, or to insert additional statements that modify the back-end database, possibly including execution of system commands.
>
> SQL injection has become a common issue with database-driven web sites. The flaw is easily detected, and easily exploited, and as such, any site or product package with even a minimal user base is likely to be subject to an attempted attack of this kind. This flaw depends on the fact that SQL makes no real distinction between the control and data planes.[42]

[40] Kinza Yasar et al., *Definition: SQL injection (SQLi)*, TechTarget (Apr. 2023), https://www.techtarget.com/searchsoftwarequality/definition/SQL-injection.

[41] *Id.*

[42] *CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')*, Common Weakness Enumeration: CWE-Individual Dictionary Definition 4.14 (Feb. 29, 2024), https://cwe.mitre.org/data/definitions/89.html.

49. SQL injection works by submitting plain text malicious SQL code as input into a web application so that a web application's server will unwittingly execute the malicious code when it processes the input.[43]

50. The malicious code may be used to reveal or alter data in the database that should not be allowed based on the limited input that the web application is expecting.[44]

51. SQL injection takes advantage of the simplicity of SQL engines, which will interpret and execute any valid SQL that is passed to them.[45]

52. For example, an SQL database may store information about customers associated with a "CustomerID" field. A form may prompt a user to enter a CustomerID so that the server can retrieve information about a customer from the database. The server would expect a user input for a "CustomerID" such as "1000." The server will then take the user input and insert it into a plain text SQL query that compares the table column "CustomerID" to the input of "1000" and return any table rows for which the statement "CustomerID=1000" is true. The query may look like this: "SELECT name, address, account_number FROM customers WHERE CustomerID=1000." This query would then be parsed and executed by the SQL engine to "select" the data fields "name, address, account_number" for any records "where" the "CustomerID" is equal to 1000. But the structure of this query is vulnerable to SQL injection because any user input is inserted directly into the plain text SQL query (*e.g.*, the user input "1000"). So, if instead of just "1000," the user input is "1000 OR 1=1," then the new query would look like this: "SELECT name, address, account_number FROM customers WHERE CustomerID=1000 OR 1=1." Rather than retrieving records where the CustomerID is 1000, this query will return any rows in which

[43] Yasar, *supra* note 40.

[44] *Id.*

[45] *Id.*

the statement "CustomerID=1000 OR 1=1" is true. Because "1=1" is always true, this statement is true for all rows in the table, regardless of whether the CustomerID for the row is equal to 1000, and therefore all rows will be returned. Depending on the design of the server, instead of being shown data from the row associated with the CustomerID of 1000, the user would be shown the first row of the table, or potentially all rows of the table, which the user may not be authorized to view. This is a rudimentary example of how SQL injection can cause a server to provide or alter more data than intended or than the user is authorized to access.[46]

53. SQL injection may also involve other SQL commands that can completely change the nature of the original query so the user can access or alter any information throughout the database.[47]

> Consider the following code that concatenates user input with SQL syntax:
>
> ```
> $name = $_REQUEST['name'];
>
> $email = $_REQUEST['email'];
>
> $sql = "INSERT INTO CustomerTable (Name,
> Email) VALUES ('$name', '$email')";
> ```
>
> Now suppose a user enters the following data:
>
> 
>
>
> The resulting SQL query (defined by $sql) is the following:
>
> ```
> INSERT INTO CustomerTable (Name, Email)
> VALUES ('Brian', 'bswan@microsoft.com');
> ```

[46] *Id.*

[47] *How and Why to Use Parameterized Queries*, Microsoft (Mar. 23, 2019), https://techcommunity.microsoft.com/t5/sql-server-blog/how-and-why-to-use-parameterized-queries/ba-p/383483.

```
DROP TABLE CustomerTable; PRINT
'Gotcha!'--')
```

54. In the above example, the user input fields "name" and "email" are inserted directly into an SQL query that will then insert those values into the table "CustomerTable." However, in the "email" form input, the user put a semi-colon—the symbol for the end of an SQL query—and then continued with a completely new SQL query: "DROP TABLE CustomerTable." A "DROP" command will delete the referenced table. When this user input is concatenated with the SQL statement and executed by the SQL engine, the table "CustomerTable" will be deleted from the database. Other commands could be used in a similar manner to alter the database, such as INSERT or UPDATE.[48]

55. SQL injection only works when a server receiving user input "trusts" that user input and enters it directly into a plain text SQL statement to be parsed and executed by the database.[49]

56. It is bad practice to trust any user input, even from authorized and trusted users, because any input can contain unexpected characters or SQL code that would then be passed directly to the database.[50]

57. Rather, user input should be validated and "sanitized" to ensure it does not contain any prohibited characters or SQL commands and matches the format expected by the server.[51]

58. In the above example, if the server were programmed to validate user input when querying the CustomerID field to ensure that any input is just a four-digit number, then when the

[48] *Id.*

[49] Yasar, *supra* note 40.

[50] *Id.*; *see also Deserialization risks in use of BinaryFormatter and related types*, Microsoft Build: Learn .NET (Apr. 4, 2023), https://learn.microsoft.com/en-us/dotnet/standard/serialization/binaryformatter-security-guide.

[51] *AO3:2021 - Injection*, Open Worldwide Application Sec. Project: OWASP Top 10 (2021), https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html#defense-option-4-strongly-discouraged-escaping-all-user-supplied-input.

server receives the input "1000 OR 1=1," the server would see that this string is not a four-digit number, reject it, and not insert the plain text input into the SQL query, thus preventing the SQL injection.[52]

59. Another common method for sanitizing user input is to "escape" special characters so they are interpreted by the SQL parser as plain text instead of SQL code.[53]

60. An escape function, when applied to a user input string, will replace special characters with neutral characters that the SQL parser will not interpret as SQL code. For example, an escape function may cause special characters to be preceded by a backslash ("\"), which signals to the SQL parser that the succeeding character should be interpreted as a plain text string, not as SQL code.[54]

61. Because escaping is a fairly rudimentary way to sanitize user input and only applies to certain characters, it cannot guarantee that SQL injection can be prevented in all cases.[55]

62. The antiquated manner of constructing SQL statements—concatenating SQL code with plain text user input—is vulnerable to SQL injection because user input might contain SQL code, so any malicious code in the user input is treated as valid SQL.[56]

---

[52] Yasar, *supra* note 40.

[53] *Defense Option 4: STRONGLY DISCOURAGED: Escaping All User-Supplied Input*, OWASP Cheat Sheet Series: SQL Injection Prevention Cheat Sheet, https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html#defense-option-4-strongly-discouraged-escaping-all-user-supplied-input (last visited Apr. 26, 2024).

[54] *STRING_ESCAPE (Transact-SQL)*, Microsoft Build: Learn .NET (Jun. 1, 2023), https://learn.microsoft.com/en-us/sql/t-sql/functions/string-escape-transact-sql.

[55] *Defense Option 4*, *supra* note 53.

[56] *How to prevent SQL Injection Vulnerabilities: How Prepared Statements Work*, Sec. Journey: Blog (Feb. 11, 2020), https://www.securityjourney.com/post/how-to-prevent-sql-injection-vulnerabilities-how-prepared-statements-work.

63. Modern and secure SQL databases, and the programming languages that interact with them, have basic tools built in called "parameterized" or "prepared" statements that can make SQL injection impossible when used properly.[57]

64. Use of parameterized statements separates SQL statements from plain text user input by performing different functions with each. The SQL engine first compiles a pre-written SQL query with defined placeholders for user input. The SQL engine then inserts the plain text user input into those placeholders. The interpretation of SQL and user input in separate steps ensures that SQL is interpreted as SQL and user input is interpreted as plain text. Therefore, even if malicious code is inputted, it cannot be interpreted and executed as SQL code, but rather, is always treated as plain text.[58]

65. The following example using the PHP programming language illustrates how parameterized statements easily separate code from input to prevent SQL injection[59]:

```
$stmt = $mysqli->prepare("SELECT * FROM
users WHERE user = ? AND password = ?");

$stmt->bind_param("ss", $username,
$password);

$stmt->execute();
```

66. In the above example, SQL is used to select a row from the table "users" where the "user" and "password" match the user input values stored in the variables "$username" and "$password." First, the "prepare" function is used to prepare the SQL query with placeholders (question marks). Only the text within the "prepare" function is interpreted as SQL. Then the

[57] *Query Parameterization Cheat Sheet*, OWASP Cheat Sheet Series: SQL Injection Prevention Cheat Sheet, https://cheatsheetseries.owasp.org/cheatsheets/Query_Parameterization_Cheat_Sheet.html (last visited Apr. 26, 2024).

[58] *SQL Injection Prevention Cheat Sheet*, OWASP Cheat Sheet Series, https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html (last visited Apr. 26, 2024).

[59] *How to prevent SQL Injection Vulnerabilities*, *supra* note 56.

"bind_param" function is used to insert the user input—stored in the variables "$username" and "$password"—into the prepared query's predefined placeholders. User input that is binded to the prepared query is interpreted as plain text. Thus, even if malicious code were inputted into the "username" or "password" fields, the server would treat the malicious code as plain text, not as executable SQL code.[60]

67. Parameterized statements are fundamental tools for developers who code with SQL.[61]

68. Sanitizing user input and using parameterized statements are easy and common ways to ensure that SQL injection is impossible.[62]

69. Sanitizing user input and using parameterized statements are industry standards and generally recognized best practices when working with user input and SQL databases.[63]

70. SQL injection is the third most critical security risk to web applications according to the Open Worldwide Application Security Project ("OWASP"), a nonprofit foundation that sets industry standards for software security.[64]

71. SQL injection has been documented, understood, and easy to prevent since 1998.[65]

---

[60] *Id.*

[61] *SQL Injection Prevention Cheat Sheet*, *supra* note 58.

[62] Yasar, *supra* note *40*.

[63] *AO3:2021 – Injection*, *supra* note 51; *How to use the OWASP Top 10 as a standard*, Open Worldwide Application Sec. Project: OWASP Top 10 (2021), https://owasp.org/Top10/A00_2021_How_to_use_the_OWASP_Top_10_as_a_standard/.

[64] *OWASP Top 10*, Open Worldwide Application Sec. Project, https://owasp.org/www-project-top-ten/; https://owasp.org/about/ (last visited Apr. 26, 2024).

[65] Yasar, *supra* note 40.

2. .NET BinaryFormatter.Deserialize vulnerability.

72. The MOVEit Transfer software performs file uploads with code written in the .NET Framework.[66]

73. .NET is a free and open-source software framework developed and maintained by Microsoft.[67]

74. Within MOVEit Transfer's file upload code, a .NET BinaryFormatter type and a Deserialize function are used when storing and recalling files while they are in the process of being uploaded.[68]

75. BinaryFormatter is used to "[s]erialize[] and deserialize[] an object, or an entire graph of connected objects, in binary format."[69]

76. BinaryFormatter is used to save (serialize) and recall (deserialize) binary objects as exact copies and, by design, does not validate that the object is valid.[70]

77. Deserialization of untrusted user input therefore introduces risks that an object is not a well-formed or validated object, potentially containing malicious code.[71]

78. Use of the BinaryFormatter type "is a classic .NET deserialization vulnerability."[72]

---

[66] Zach Hanley, *MOVEit Transfer CVE-2023-34362 Deep Dive and Indicators of Compromise*, Horizon3.ai: Attack Blogs (Jun. 9, 2023), https://www.horizon3.ai/attack-research/attack-blogs/moveit-transfer-cve-2023-34362-deep-dive-and-indicators-of-compromise/.

[67] *Download.NET*, Microsoft: .NET, https://dotnet.microsoft.com/en-us/download (last visited Apr. 26, 2024).

[68] Hanley, *supra* note 66.

[69] *BinaryFormatter Class*, Microsoft Build: Learn .NET, https://learn.microsoft.com/en-us/dotnet/api/system.runtime.serialization.formatters.binary.binaryformatter (last visited Apr. 26, 2024).

[70] *Sterilization in .NET*, Microsoft Build: Learn .NET (Oct. 25, 2023), https://learn.microsoft.com/en-us/dotnet/standard/serialization/.

[71] *Deserialization of Untrusted Data*, Open Worldwide Application Sec. Project, https://owasp.org/www-community/vulnerabilities/Deserialization_of_untrusted_data (last visited Apr. 26, 2024).

[72] Hanley, *supra* note 66.

79. "BinaryFormatter was implemented before deserialization vulnerabilities were a well-understood threat category. As a result, the code does not follow modern best practices."[73]

80. Microsoft advises regarding use of BinaryFormatter and Deserialize[74]:

> The BinaryFormatter type is dangerous and is ***not*** recommended for data processing. Applications should stop using BinaryFormatter as soon as possible, even if they believe the data they're processing to be trustworthy. BinaryFormatter is insecure and can't be made secure.
>
> . . .
>
> Deserialization vulnerabilities are a threat category where request payloads are processed insecurely. An attacker who successfully leverages these vulnerabilities against an app can cause denial of service (DoS), information disclosure, or remote code execution inside the target app. This risk category consistently makes the OWASP Top 10.
>
> . . .
>
> As a simpler analogy, assume that calling BinaryFormatter.Deserialize over a payload is the equivalent of interpreting that payload as a standalone executable and launching it.
>
> . . .
>
> The BinaryFormatter.Deserialize method is **never** safe when used with untrusted input. We strongly recommend that consumers instead consider using one of the alternatives outlined later in this article.
>
> . . .
>
> We recommend that BinaryFormatter consumers perform individual risk assessments on their apps. It is the consumer's sole responsibility to determine whether to utilize BinaryFormatter. If you're considering using it, you should risk-assess the security, technical, reputation, legal, and regulatory consequences.

[73] *Deserialization risks in use of BinaryFormatter and related types*, *supra* note 50.

[74] *Id.*

81. "[C]alling BinaryFormatter.Deserialize over a payload is the equivalent of interpreting that payload as a standalone executable and launching it."[75]

82. An unauthorized user could therefore upload a malicious program to a server that uses the BinaryFormatter.Deserialize function, and the server would unwittingly execute the code with administrator permissions, known as remote code execution.[76]

83. Due to these critical security vulnerabilities, recent versions of .NET now flag any use of BinaryFormatter.Deserialize as an error.[77]

84. The API documentation page for BinaryFormatter immediately warns developers of the vulnerability: "BinaryFormatter serialization is obsolete and should not be used."[78]

85. Ultimately, Microsoft recommends: "Stop using BinaryFormatter in your code."[79]

86. OWASP ranked "Insecure Deserialization" as number 8 on their 2017 Top 10 list of software security vulnerabilities based on an industry survey.[80]

87. OWASP now ranks "Vulnerable and Outdated Components" as the sixth ranking web application security risk.[81]

88. The BinaryFormatter.Deserialize vulnerability has been documented, understood, and easy to prevent since at least 2017, when the tool YSoSerial.Net was developed. YsoSerial.Net is "[a] proof-of-concept tool for generating payloads that exploit unsafe .NET object

---

[75] *Id.*

[76] Hanley, *supra* note 66.

[77] *BinaryFormatter serialization methods are obsolete and prohibited in ASP.NET apps*, Microsoft Build: Learn .NET (May 17, 2023), https://learn.microsoft.com/en-us/dotnet/core/compatibility/serialization/5.0/binaryformatter-serialization-obsolete.

[78] *BinaryFormatter Class*, *supra* note 69.

[79] *BinaryFormatter serialization methods are obsolete and prohibited in ASP.NET apps*, *supra* note 77.

[80] *A8:2017-Insecure Deserialization*, Open Worldwide Application Sec. Project: OWASP Top 10 (2017), https://owasp.org/www-project-top-ten/2017/A8_2017-Insecure_Deserialization.html.

[81] *OWASP Top Ten*, *supra* note 64.

deserialization." YSoSerial.Net has 27 contributors to its open-source codebase, has been continuously maintained, and has approximately 3,000 stars on GitHub.[82]

89. Microsoft recommends use of YSoSerial.Net "for research into how adversaries attack apps that utilize BinaryFormatter."[83]

D. Cl0p exploited the MOVEit vulnerabilities to steal data from hundreds of organizations.

1. Cl0p Ransomware Gang.

90. Cl0p, also known as TA505, is a Russian cybercriminal ransomware gang.[84]

91. Emerging in February 2019, Cl0p primarily used "double extortion" tactics whereby Cl0p would hack into an organization's network, encrypt the data therein, and then exfiltrate and threaten to leak the data on the dark web. The only way for the organization to regain access to their data and prevent it from being leaked was to pay a ransom.[85]

92. In 2021, Cl0p began to rely primarily on stealing and ransoming data rather than encrypting data.[86]

93. Cl0p operates the dark website >_CLOP^_-LEAKS, on which it posts ransom demands and leaks stolen data.[87]

---

[82] pwntester (Alvaro Muñoz), *ysoserial.net*, GitHub (Oct. 17, 2023), https://github.com/pwntester/ysoserial.net.

[83] *Deserialization risks in use of BinaryFormatter and related types*, *supra* note 50.

[84] Sean Lyngaas, *Russian-speaking cyber gang claims credit for hack of BBC and British Airways employee data*, CNN (Jun. 7, 2023, 12:56 PM), https://www.cnn.com/2023/06/07/tech/clop-russia-moveit-hack-payroll-uk/index.html; Cybersecurity & Infrastructure Sec. Agency (CISA), *#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability*, Cybersecurity Advisory: Alert AA23-158A (Jun. 7, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

[85] CISA Alert AA23-158A, *supra* note 84.

[86] *Id.*

[87] Riam Kim-Mcleod, *Clop Leaks: First Wave of Victims Named*, ReliaQuest: Blog (Jul. 28, 2023, 10:00 AM), https://www.reliaquest.com/blog/clop-leaks-first-victims/.

94. Cl0p "conducted zero-day-exploit-driven campaigns against Accellion File Transfer Appliance (FTA) devices in 2020 and 2021, and Fortra/Linoma GoAnywhere MFT servers in early 2023."[88]

95. "Beyond CL0P ransomware, TA505 is known for frequently changing malware and driving global trends in criminal malware distribution. Considered to be one of the largest phishing and malspam distributors worldwide, TA505 is estimated to have compromised more than 3,000 U.S.-based organizations and 8,000 global organizations."[89]

2. Exploiting MOVEit Transfer vulnerabilities.

96. MOVEit Transfer was defective and vulnerable to SQL injection because it did not sanitize user input, use parameterized statements, or follow other industry data security standards to prevent malicious code from being remotely inputted into its database.[90]

97. Analysis of the "guestaccess.aspx" login page within the MOVEit Transfer code revealed an "SQL query [made] from a concatenated string of several arguments passed in"[91]:

```
SELECT Username, Permissions, LoginName, Email
FROM users WHERE InstID=9389 AND Deleted=0 AND
(Email='<EmailAddress>' OR Email LIKE
(%EscapeLikeForSQL(<EmailAddress>)) or Email
LIKE (EscapeLikeForSQL(<EmailAddress>));
```

98. There are three comparisons in the SQL query that compare a user-inputted value "<EmailAddress>" to a table column "Email."[92]

[88] CISA Alert AA23-158A, *supra* note 84.

[89] CISA Alert AA23-158A, *supra* note 84.

[90] Hanley, *supra* note 66.

[91] *Id.*

[92] *Id.*

99. Two of the comparisons escape the user input before comparing it to the table using the function "EscapeLikeForSQL."[93]

100. But the other comparison does not escape the user input, instead simply comparing the user input "<EmailAddress>" to the table column "Email" one-to-one[94]:

```
Email='<EmailAddress>'
```

101. An unauthorized user could access a MOVEit Transfer database by inputting malicious code into a form field that prompts a user to enter an email address, and the malicious code would be inputted into the above plain text SQL query where the unescaped "<EmailAddress>" user input is included.[95]

102. The malicious code would be executed because the MOVEit Transfer software did not sanitize the user input nor did it prepare the SQL query as a parameterized statement to separate code execution from user input.[96]

103. This vulnerability gives unauthorized users "the ability to read and write any data within the MOVEit database."[97]

104. The unauthorized user can then pose as a logged-in user by sending a request to the "guestaccess.aspx" page of the MOVEit Transfer server with fake credentials embedded with malicious SQL code.[98]

---

[93] *Id.*

[94] *Id.*

[95] *Id.*

[96] *Id.*

[97] *Id.*

[98] *Id.*

105. When the server attempts to authenticate the fake credentials by executing the above query, it will execute the malicious SQL code.[99] The defective design of MOVEit allows a hacker to exploit this vulnerability, which results in automatic execution of the malicious SQL code.

106. The unauthorized user then leverages a "federated login flow," which is a system that allows users to log-in to the MOVEit Transfer server using credentials for a third-party account, such as a Microsoft Outlook account. The federated login flow works by sending a JSON web token to the "/api/v1/auth/token" API endpoint of the MOVEit Transfer server containing a signature and a link to a trusted certificate to verify the credentials from the third-party account.[100]

107. The SQL injection can be used to configure the MOVEit Transfer server to accept a federated login certificate from an untrusted source.[101]

108. The unauthorized user can then send a JSON web token to the server with a fake certificate and "obtain an access token for the sysadmin user."[102]

109. Once the unauthorized user has administrator permissions, they can access MOVEit Transfer functions for uploading and downloading files.[103]

110. The unauthorized user can then download files from the MOVEit Transfer server through the MOVEit Transfer client, web app, or API.[104]

---

[99] *Id.*

[100] *Id.*

[101] *Id.*

[102] *Id.*

[103] *Id.*

[104] *Id.*

111. With root access to the server—not merely administrator permissions within the MOVEit Transfer software—the unauthorized user can compress and bulk download files saved on the server more easily and efficiently.[105]

112. Gaining root access to the server involves taking advantage of a vulnerability in the file upload API endpoint at "/api/v1/folders/<folder_id>/files?uploadType=resumable&fileId=<file_id>."[106]

113. "When initiating [a] file upload [through MOVEit Transfer], you can optionally provide a Comment. This comment is encrypted with that organization specific key."[107]

114. The unauthorized user sends a request to the MOVEit Transfer file upload endpoint, which logs the upload request in the database. The unauthorized user does not attempt to upload a real file, but rather includes in their request a "comment" to be associated with the file upload. The server takes the comment, encrypts it using the encryption key, and stores it in the database.[108]

115. The result is an entry in the MOVEit Transfer database for a paused file upload containing the encrypted comment[109]:

Figure 4

```
mysql> SELECT * FROM fileuploadinfo;
+-----------+--------------------------------------------+--------------------+-----------------+-------+
| FileID    | Comment                                    | XferID             | BytesTransferred | State |
+-----------+--------------------------------------------+--------------------+-----------------+-------+
| 965667160 | @%!4QBbFxKJMyTwaNCzjoBCqXm8L/uReX9CqGkp8g== | 4237971835089001547 |               0 | NULL  |
+-----------+--------------------------------------------+--------------------+-----------------+-------+
1 row in set (0.00 sec)
```

[105] *Id.*

[106] *Id.*

[107] *Id.*

[108] *Id.*

[109] *Id.*

116. The unauthorized user then uses SQL injection to move the value in the "Comment" column to the "State" column.[110]

117. The unauthorized user can make the "Comment" a serialized malicious program, which can be accomplished easily with a tool such as YSoSerial.Net.[111]

118. When the unauthorized user prompts the server to resume the file upload, the server decrypts the "State" column—now containing the unauthorized user's serialized malicious program—into a .NET BinaryFormatter type and performs the function Deserialize on it.[112]

119. Because of the way that the BinaryFormatter.Deserialize function works, as outlined above, this action effectively executes the malicious code that was written into the "State" column.[113]

120. The unauthorized user's malicious code is executed as a .NET program running at the root level rather than by the SQL engine running only within the database. The code therefore has access to the same context as a .NET program, *i.e.*, the entire server and all files on the server, not just the MOVEit Transfer software.[114]

121. Cl0p used the SQL injection and BinaryFormatter.Deserialize vulnerabilities to install a malicious web shell called LEMURLOOT on MOVEit Transfer servers.[115]

---

[110] *Id.*

[111] *Id.*

[112] *Id.*

[113] *Id.*

[114] *Id.*; *Deserialization risks in use of BinaryFormatter and related types*, *supra* note 50.

[115] Nader Zaveri et al., *Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft*, Mandiant: Blog (Apr. 3, 2024), https://www.mandiant.com/resources/blog/zero-day-moveit-data-theft.

122. A web shell is a program that allows a user to execute commands on a web server without having physical access to it.[116]

123. LEMURLOOT was written specifically to compromise MOVEit Transfer servers, evidenced by its use of MOVEit-specific code libraries.[117]

124. LEMURLOOT "authenticates incoming connections via a hard-coded password and can run commands that will download files from the MOVEit Transfer system, extract its Azure system settings, retrieve detailed record information, create and insert a particular user, or delete this same user."[118]

125. Because LEMURLOOT can access the encryption keys that are saved on the server, it can decrypt files that MOVEit Transfer encrypted on the server.[119]

126. LEMURLOOT therefore allowed unauthorized users to decrypt, compress, and bulk download all files saved on MOVEit Transfer servers.[120]

127. LEMURLOOT can also access files containing server credentials, such as Azure Storage Blob information.[121]

128. LEMURLOOT was given the file name "human2.aspx" to mimic the file name of the legitimate MOVEit Transfer file "human.aspx" and avoid detection.[122]

---

[116] Cybersecurity & Infrastructure Sec. Agency (CISA), *Compromised Web Servers and Web Shells - Threat Awareness and Guidance*, Alert: TA15-314A (Aug. 9, 2017), https://www.cisa.gov/news-events/alerts/2015/11/10/compromised-web-servers-and-web-shells-threat-awareness-and-guidance.

[117] CISA Alert AA23-158A, *supra* note 84.

[118] Zaveri, *supra* note 115.

[119] *Id.*

[120] *Id.*

[121] *Id.*

[122] Dan Goodin, *Mass exploitation of critical MOVEit flaw is ransacking orgs big and small*, Ars Technica (Jun. 5, 2023, 10:05 PM) https://arstechnica.com/information-technology/2023/06/mass-exploitation-of-critical-moveit-flaw-is-ransacking-orgs-big-and-small/.

129. Below is an example log detailing the server requests performed in the attacks, ultimately leading to successful access to the LEMURLOOT web shell at "human2.aspx"[123]:

Figure 5

```
2023-05-28 20:58:19 GET  /
2023-05-28 20:58:19 GET  /moveitisapi/moveitisapi.dll action=capa
2023-05-28 20:58:20 POST /moveitisapi/moveitisapi.dll action=m2
2023-05-28 20:58:21 POST /guestaccess.aspx
2023-05-28 20:58:26 POST /guestaccess.aspx
2023-05-28 20:58:26 POST /moveitisapi/moveitisapi.dll action=m2
2023-05-28 20:58:28 POST /guestaccess.aspx
2023-05-28 20:58:28 POST /api/v1/token
2023-05-28 20:58:28 GET  /api/v1/folders
2023-05-28 20:58:29 POST /api/v1/folders/582151639/files uploadType=resumable
2023-05-28 20:58:29 POST /moveitisapi/moveitisapi.dll action=m2
2023-05-28 20:58:30 POST /guestaccess.aspx
2023-05-28 20:58:32 PUT  /api/v1/folders/582151639/files uploadType=resumable&fileId=962420679
2023-05-28 20:58:32 POST /moveitisapi/moveitisapi.dll action=m2
2023-05-28 20:58:34 POST /guestaccess.aspx
2023-05-28 20:58:40 GET  /human2.aspx  {FAIL}
2023-05-28 20:59:19 GET  /human2.aspx  {FAIL}
2023-05-28 21:00:03 GET  /human2.aspx  {SUCCESS}
```

130. Data theft can occur within minutes of deployment of the web shell.[124]

131. Though MOVEit Transfer's SQL injection vulnerability was exploited to provide unauthorized users with administrative permissions within the MOVEit Transfer software, these permissions would still limit the user to the capabilities of the MOVEit Transfer software—*i.e.*, the user would still only be able to access and download files in the manner that the MOVEit Transfer software is designed, which could be slow and tedious. The addition of the LEMURLOOT web shell, by exploiting the BinaryFormatter.Deserialize vulnerability, substantially increased the speed and efficiency of the attacks because the web shell could decrypt, compress, and bulk download files directly from the server, without having to work within the MOVEit Transfer software.[125]

---

[123] Scott Downie et al., *Clop Ransomware Likely Sitting on MOVEit Transfer Vulnerability (CVE-2023-34362) Since 2021*, Kroll (Jun. 8, 2023), https://www.kroll.com/en/insights/publications/cyber/clop-ransomware-moveit-transfer-vulnerability-cve-2023-34362.

[124] Zaveri, *supra* note 115.

[125] *Id.*

132. All versions of MOVEit Transfer are subject to these critical vulnerabilities—which have long been understood and documented—confirming that the vulnerabilities existed in MOVEit Transfer for years without being discovered or fixed in subsequent versions.[126]

133. MOVEit versions as old as 2020 (and possibly even earlier) were ultimately patched to fix these critical vulnerabilities after the Data Breach, further confirming that Progress supports and permits clients to use versions of the software that are many years old and were developed with these vulnerabilities.[127]

134. These vulnerabilities and attack vectors have been widely reported and tested by multiple third parties, further verifying that the Data Breach occurred in substantially the same manner as detailed above.[128]

3. Zero-Day.

135. MOVEit Transfer, as a popular, highly available, and widely-distributed software installed on individual customers' servers—and "thus not easily patched"—and accessible over the Internet, presented a unique opportunity for hackers because public-facing MOVEit Transfer server web applications can be found easily by searching the Internet, and numerous MOVEit Transfer customers could be attacked simultaneously—and automatically—with the same exact strategy.[129]

---

[126] *MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362)*, Progress: Community (Jun. 16, 2023), https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023.

[127] *Id.*

[128] Zaveri, *supra* note 115; Hanley, *supra* note 66; John Hammond, *MOVEit Transfer Critical Vulnerability CVE-2023-34362 Rapid Response*, Huntress: Blog (June 1, 2023), https://www.huntress.com/blog/moveit-transfer-critical-vulnerability-rapid-response.

[129] Joe Slowik, *Move It on Over: Reflecting on the MOVEit Exploitation*, Huntress: Blog (Jul. 7, 2023), https://www.huntress.com/blog/move-it-on-over-reflecting-on-the-moveit-exploitation.

136. Because MOVEit Transfer software is installed on customers' servers rather than Progress servers, Cl0p scanned the Internet looking for servers with publicly accessible MOVEit Transfer login pages, denoted by a page called "human.aspx."[130]

137. Traffic from known Cl0p IP addresses began scanning the Internet for MOVEit Transfer login pages, attempting to discover vulnerable MOVEit Transfer installations, as early as July 2021.[131]

138. Cl0p had therefore been developing this strategy and planning their targets since 2021, ready to inflict the maximum amount of damage in a short amount of time.[132]

139. Using a strategy similar to that outlined above, Cl0p was able to exploit vulnerabilities in the MOVEit Transfer software to gain access to each server's files without detection.[133]

140. It is not known when Cl0p began deploying this strategy, but the earliest publicly available evidence shows that Cl0p began installing LEMURLOOT on MOVEit Transfer servers by May 27, 2023.[134]

141. May 27, 2023, coincided with Memorial Day weekend, consistent with a common strategy employed by hackers to launch attacks on holiday weekends when victims may be unable to respond.[135]

---

[130] Matthew Remacle, *Progress' MOVEit Transfer Critical Vulnerability: CVE-2023-34362*, GreyNoise: Blog (June 1, 2023), https://www.greynoise.io/blog/progress-moveit-transfer-critical-vulnerability.

[131] Downie, *supra* note 123.

[132] *Id.*

[133] Zaveri, *supra* note 115.

[134] *Id.*

[135] Downie, *supra* note 123.

142. Because the MOVEit Transfer software was not designed to discover or defend against this type of attack, it initially went undetected.[136]

143. Such attacks are called "zero-day" attacks because the specific flaw is exploited before the developer is aware of it—*i.e.*, the developer has had zero days to release a patch.[137]

144. Because data theft can occur within minutes of deployment of LEMURLOOT, Cl0p was able to simultaneously attack thousands of MOVEit Transfer servers and steal troves of data in a relatively short time before detection.[138]

4. Discovery of the Data Breach.

145. On May 28, 2023, "the MOVEit technical support team received initial customer calls indicating suspicious activity."[139]

146. A malicious "staged exploit" was discovered and removed from three MOVEit Cloud clusters on May 30, 2023.[140]

147. MOVEit Cloud was temporarily shut down on May 30 and May 31, 2023;[141] MOVEit Cloud service was restored later on May 31, 2023.[142]

---

[136] Zaveri, *supra* note 115.

[137] *What is a Zero-day Attack? - Definition and Explanation*, Kaspersky, https://usa.kaspersky.com/resource-center/definitions/zero-day-exploit (last visited Apr. 26, 2024).

[138] Zaveri, *supra* note 115.

[139] *Status of the May 2023 security vulnerability and defensive outage of MOVEit Cloud*, Progress: Community (June 1, 2023), https://community.progress.com/s/article/MOVEit-Cloud-Info-Regarding-Critical-Vulnerability-May-2023.

[140] *Id.*

[141] *Id.*

[142] *Id.*

148. On May 31, 2023, Progress announced the discovery of an "SQL injection vulnerability . . . in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database."[143]

149. Progress found that, "depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database and execute SQL statements that alter or delete database elements."[144]

150. Progress found that the vulnerability was "exploited in the wild in May and June 2023."[145]

151. The vulnerability affected "[a]ll MOVEit Transfer versions."[146]

152. The Data Breach was further publicized by June 5, 2023, when multiple companies began coming forward to announce that their MOVEit Transfer servers were compromised.[147]

153. Signs of a breach in a customer's MOVEit Transfer database are evidenced by unauthorized entries in the "userexternaltokens," "trustedexternaltokenproviders," and "hostpermits" tables whereby the sysadmin was obtained, as well as log entries for the endpoints that the unauthorized users utilized[148]:

a. <InstallDir>/Logs/DMZ_WebApi.log when requests are made to /api/v1/ endpoints

[143] *Id.*

[144] *Id.*

[145] *Id.*

[146] *Id.*

[147] Matt Kapko, *Worries mount for MOVEit vulnerability, as likelihood of compromise expands*, Cybersecurity Drive (June 5, 2023), https://www.cybersecuritydive.com/news/moveit-vulnerability-worries-mount/652035/.

[148] Zaveri, *supra* note 115.

b. <InstallDir>/Logs/DMZ_WEB.log when requests are made to /guestaccess.aspx and relayed messages to /machine2.aspx

c. <InstallDir>/Logs/DMZ_ISAPI.log when requests are made to /moveitisapi/moveitisapi.dll?action=m2

154. Though a malicious "staged exploit" was discovered on MOVEit Cloud clusters, Progress reported that there was no evidence that the exploit was activated or that MOVEit Cloud data was compromised.[149]

155. Progress has not stated whether MOVEit Cloud utilizes the same code that was subject to the same vulnerabilities as MOVEit Transfer or if MOVEit Cloud was developed and maintained to not be vulnerable to the same type of attacks as MOVEit Transfer.

E. Progress's May 31 patch that came too late.

1. Mitigating and patching the MOVEit vulnerabilities.

156. On May 31, 2023, Progress published its finding of an "SQL injection vulnerability . . . in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database and execute SQL statements that alter or delete database elements."[150]

157. The vulnerability was given the unique identifier CVE-2023-34362 in the National Vulnerability Database maintained by the United States National Institute of Standards and Technology ("NIST").[151]

---

[149] *Status of the May 2023 security vulnerability and defensive outage of MOVEit Cloud*, *supra* note 139.

[150] *MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362)*, *supra* note 126.

[151] NIST, *Progress MOVEit Transfer SQL Injection Vulnerability (CVE-2023-34362) Detail*, Nat'l Vulnerability Database (June 23, 2023), https://nvd.nist.gov/vuln/detail/CVE-2023-34362.

158. The vulnerability was given a severity rating under the Common Vulnerability Scoring System of 9.8 out of 10, signifying that the vulnerability is near the highest level of severity, or "critical."[152]

159. The vulnerability was marked with a Common Weakness Enumeration code CWE-89, for "Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')."[153]

160. Progress recommended the following steps to mitigate the damage caused by the vulnerability until a patch could be installed[154]:

a. "Disable all HTTP and HTTPs traffic to your MOVEit Transfer environment"

b. "Delete Unauthorized Files and User Accounts"

c. "Reset service account credentials for affected systems and MOVEit Service Account"

161. Progress published a patch on May 31, 2023, with updated code that Progress claims will prevent further SQL injection attacks and remote code execution as outlined above, stating[155]:

> Progress has discovered a vulnerability in MOVEit Transfer that could lead to escalated privileges and potential unauthorized access to the environment. If you are a MOVEit Transfer customer, it is extremely important that you take immediate action as noted below in order to help protect your MOVEit Transfer environment.

162. Cybersecurity firm Huntress investigated the CVE-2023-34362 attack vector and discovered another SQL injection attack vector, which was assigned CVE-2023-35036.[156]

---

[152] *Id.*

[153] *CWE-89*, *supra* note 42.

[154] *MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362)*, *supra* note 126.

[155] Goodin, *supra* note 122.

[156] Hammond, *supra* note 128.

163. Progress published another patch on June 9, 2023, for CVE-2023-35036, again with the CWE-89 SQL injection vulnerability, stating[157]:

> SQL Injection (CVE-2023-35036) In Progress MOVEit Transfer versions released before 2021.0.7 (13.0.7), 2021.1.5 (13.1.5), 2022.0.5 (14.0.5), 2022.1.6 (14.1.6), 2023.0.2 (15.0.2), multiple SQL injection vulnerabilities have been identified in the MOVEit Transfer web application that could allow an un-authenticated attacker to gain unauthorized access to the MOVEit Transfer database. An attacker could submit a crafted payload to a MOVEit Transfer application endpoint which could result in modification and disclosure of MOVEit database content. All versions of MOVEit Transfer are affected by this vulnerability. Patches for this vulnerability are available for supported versions and are listed in the Recommended Remediation section.

164. Progress published another patch on June 15, 2023, for yet another newly discovered attack vector, CVE-2023-35708, again with the CWE-89 SQL injection vulnerability, stating[158]:

> Progress has discovered a vulnerability in MOVEit Transfer that could lead to escalated privileges and potential unauthorized access to the environment. If you are a MOVEit Transfer customer, it is extremely important that you take immediate action as noted below in order to help protect your MOVEit Transfer environment. In Progress MOVEit Transfer versions released before 2021.0.8 (13.0.8), 2021.1.6 (13.1.6), 2022.0.6 (14.0.6), 2022.1.7 (14.1.7), 2023.0.3 (15.0.3), a SQL injection vulnerability has been identified in the MOVEit Transfer web application that could allow an un-authenticated attacker to gain unauthorized access to the MOVEit Transfer database. An attacker could submit a crafted payload to a MOVEit Transfer application endpoint which could result in modification and disclosure of MOVEit database content.

---

[157] *MOVEit Transfer Critical Vulnerability – CVE-2023-35036*, Progress: Community (June 9, 2023), https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-CVE-2023-35036-June-9-2023; *CVE-2023-34362 Detail*, *supra* note 151.

[158] *MOVEit Transfer Critical Vulnerability – CVE-2023-35708*, Progress: Community (Jun. 15, 2023), https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-15June2023; *CVE-2023-34362 Detail*, *supra* note 151.

165. On July 6, 2023, Progress released another service pack containing patches for three more newly discovered vulnerabilities in MOVEit Transfer[159]—two involving SQL injection (CWE-89)[160] and one involving Improper Handling of Exceptional Conditions (CWE-755).[161]

166. On September 20, 2023, Progress released another service pack containing patches for three more newly discovered vulnerabilities in MOVEit Transfer[162]—two involving SQL injection (CWE-89)[163] and one involving Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (CWE-79).[164]

167. On November 29, 2023, Progress released another service pack containing patches for two more newly discovered vulnerabilities in MOVEit Transfer[165]—one involving Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (CWE-79)[166] and one involving Improper Privilege Management (CWE-269).[167]

---

[159] *MOVEit Transfer Service Pack – (July 2023)*, Progress: Community (July 6, 2023), https://community.progress.com/s/article/MOVEit-Transfer-Service-Pack-July-2023.

[160] NIST, *CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (CVE-2023-36932) Detail*, Nat'l Vulnerability Database (July 12, 2023), https://nvd.nist.gov/vuln/detail/CVE-2023-36932; NIST, *CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (CVE-2023-36934) Detail*, Nat'l Vulnerability Database (July 10, 2023), https://nvd.nist.gov/vuln/detail/CVE-2023-36934.

[161] NIST, *CWE-755 Improper Handling of Exceptional Conditions (CVE-2023-36933) Detail*, Nat'l Vulnerability Database (July 12, 2023), https://nvd.nist.gov/vuln/detail/CVE-2023-36933.

[162] *MOVEit Transfer Service Pack – (July 2023)*, *supra* note 159.

[163] NIST, *CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (CVE-2023-42660) Detail*, Nat'l Vulnerability Database (Aug. 22, 2023), https://nvd.nist.gov/vuln/detail/CVE-2023-42660; NIST, *CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (CVE-2023-40043) Detail*, Nat'l Vulnerability Database (Aug. 22, 2023), https://nvd.nist.gov/vuln/detail/CVE-2023-40043.

[164] NIST, *CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (CVE-2023-42656) Detail*, Nat'l Vulnerability Database (Aug. 22, 2023), https://nvd.nist.gov/vuln/detail/CVE-2023-42656.

[165] *MOVEit Transfer Service Pack - (Nov. 2023)*, Progress: Community (Nov. 29, 2023), https://community.progress.com/s/article/MOVEit-Transfer-Service-Pack-November-2023.

[166] NIST, *CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (CVE-2023-6217) Detail*, Nat'l Vulnerability Database (Dec. 5, 2023), https://nvd.nist.gov/vuln/detail/CVE-2023-6217.

[167] NIST, *CWE-269 Improper Privilege Management (CVE-2023-6218) Detail*, Nat'l Vulnerability Database (Dec. 5, 2023), https://nvd.nist.gov/vuln/detail/CVE-2023-6218.

168. On January 17, 2024, Progress released another service pack containing a patch for another newly discovered vulnerability in MOVEit Transfer[168] involving Improper Input Validation (CWE-20).[169]

169. On March 21, 2024, Progress released another service pack containing a patch for another newly discovered vulnerability in MOVEit Transfer[170] involving Insufficient Logging (CWE-778).[171]

170. Patches are only effective after customers are informed about them and install them, as "[c]ybercriminals often probe systems and networks to see if they are out of date and missing a security patch."[172]

171. Since the discovery of the MOVEit Transfer SQL injection vulnerabilities, Progress has continued to be plagued with critical vulnerabilities found in its other software products as it reviews outdated and insecure code[173]:

> **WS_FTP Server Critical Vulnerability (September 2023)**
>
> The WS_FTP team recently discovered vulnerabilities in the WS_FTP Server Ad hoc Transfer Module and in the WS_FTP Server manager interface. All versions of WS_FTP Server are affected by these vulnerabilities. We have addressed these issues

[168] *MOVEit Transfer Service Pack – (Jan. 2024)*, Progress: Community (Jan. 17, 2024), https://community.progress.com/s/article/MOVEit-Transfer-Service-Pack-January-2024.

[169] NIST, *CWE-20 Improper Input Validation & NVD-CWE-Info Insufficient Information (CVE-2024-0396) Detail*, Nat'l Vulnerability Database (Jan. 1, 2024), https://nvd.nist.gov/vuln/detail/CVE-2024-0396.

[170] *MOVEit Transfer Service Pack (March 2024)*, Progress: Community (Mar. 21, 2024), https://community.progress.com/s/article/MOVEit-Transfer-Service-Pack-March-2024.

[171] NIST, *CWE-778 Insufficient Logging (CVE-2024-2291) Detail*, Nat'l Vulnerability Database (Mar. 20, 2024), https://nvd.nist.gov/vuln/detail/CVE-2024-2291.

[172] Arya Arun, *Cyber Security Vulnerability: Signs Your Network & Systems May Be Weak*, StickmanCyber (July 21, 2022), https://www.stickmancyber.com/cybersecurity-blog/cyber-security-vulnerability-signs-your-network-systems-may-be-weak.

[173] *Critical Alerts*, Progress: Community, https://community.progress.com/s/global-search/%40uri#t=KnowledgeBase&sort=date%20descending&f:@sfarticletypec=[Critical_Alert] (last visited Apr. 26, 2024).

and have made version-specific hotfixes available for customers to remediate them.[174]

* * *

WS_FTP Server Service Pack (November 2023)

This article contains the details of the specific updates within the WS_FTP Server November 2023 Service Pack. The Service Pack contains fixes for one newly disclosed CVE described below. Progress Software highly recommends you apply this Service Pack for product updates and security improvements. For Service Pack content, please review the Service Pack Release Notes and this knowledgebase article carefully to help you plan when it is appropriate to apply to your environments.[175]

* * *

Important Progress OpenEdge Critical Alert for Progress Application Server in OpenEdge (PASOE) - Arbitrary File Upload Vulnerability in WEB Transport

The WEB transport in PASOE has support for file uploads across all web handlers and all web handlers are affected including the built-in handlers. The expected behavior is that file upload is disabled by default since the value for the "fileUploadDirectory" property in the openedge.properties file is blank. However, this default property setting allows access to all directories for the user account that started the PASOE instance. If these directories have write permission, the system running PASOE is vulnerable to a malicious file upload on the system (Linux) or on the root drive (Windows). An attacker with the unexpected ability to upload to the system running PASOE could then launch a wider scale attack.[176]

* * *

[174] *WS_FTP Server Critical Vulnerability (Sept. 2023)*, Progress: Community (Oct. 20, 2023), https://community.progress.com/s/article/WS-FTP-Server-Critical-Vulnerability-September-2023.

[175] *WS_FTP Server Service Pack (Nov. 2023)*, Progress: Community (Nov. 7, 2023), https://community.progress.com/s/article/WS-FTP-Server-Service-Pack-November-2023.

[176] *Important Progress OpenEdge Critical Alert for Progress Application Server in OpenEdge (PASOE) - Arbitrary File Upload Vulnerability in WEB Transport*, Progress: Community (Jan. 18, 2024), https://community.progress.com/s/article/Important-Progress-OpenEdge-Critical-Alert-for-Progress-Application-Server-in-OpenEdge-PASOE-Arbitrary-File-Upload-Vulnerability-in-WEB-Transport.

> **Important Security Update for OpenEdge Authentication Gateway and AdminServer**
>
> When the OpenEdge Authentication Gateway (OEAG) is configured with an OpenEdge Domain that uses the OS local authentication provider to grant user-id and password logins on operating platforms supported by active releases of OpenEdge, a vulnerability in the authentication routines may lead to unauthorized access on attempted logins.
>
> Similarly, when an AdminServer connection is made by OpenEdge Explorer (OEE) and OpenEdge Management (OEM), it also utilizes the OS local authentication provider on supported platforms to grant user-id and password logins that may also lead to unauthorized login access.[177]

172. These more recent critical vulnerabilities involved the following Common Weakness Enumerations, as reported by NIST, some of which are the same as the SQL injection and deserialization vulnerabilities found in MOVEit Transfer:

a. CVE-2023-40044: CWE-502 Deserialization of Untrusted Data[178]

b. CVE-2023-42657: CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')[179]

c. CVE-2023-40045: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')[180]

d. CVE-2023-40046: CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')[181]

---

[177] *Important Security Update for OpenEdge Authentication Gateway and AdminServer*, Progress: Community (Feb. 27, 2024), https://community.progress.com/s/article/Important-Critical-Alert-for-OpenEdge-Authentication-Gateway-and-AdminServer.

[178] NIST, *CWE*-502 *Deserialization of Untrusted Data (CVE-2023-40044) Detail*, Nat'l Vulnerability Database (Oct. 12, 2023), https://nvd.nist.gov/vuln/detail/CVE-2023-40044.

[179] NIST, *CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (CVE-2023-42657) Detail*, Nat'l Vulnerability Database (Aug. 29, 2023), https://nvd.nist.gov/vuln/detail/CVE-2023-42657.

[180] NIST, *CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (CVE-2023-40045) Detail*, Nat'l Vulnerability Database (Aug. 27, 2023), https://nvd.nist.gov/vuln/detail/CVE-2023-40045.

[181] NIST, *CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), CVE-2023-40046) Detail*, Nat'l Vulnerability Database (Aug. 27, 2023), https://nvd.nist.gov/vuln/detail/CVE-2023-40046.

e. CVE-2023-40047: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')[182]

f. CVE-2023-40048: CWE-352 Cross-Site Request Forgery (CSRF)[183]

g. CVE-2022-27665: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')[184]

h. CVE-2023-40049: CWE-200 Exposure of Sensitive Information to an Unauthorized Actor[185]

i. CVE-2023-42659: CWE-434 Unrestricted Upload of File with Dangerous Type[186]

j. CVE-2023-40051: CWE-434 Unrestricted Upload of File with Dangerous Type[187]

k. CVE-2024-1403: CWE-305 Authentication Bypass by Primary Weakness[188]

173. These critical vulnerabilities show that Progress continues to employ poorly written, outdated, and insecure code in its software, without updating outdated code, checking for known or newly discovered vulnerabilities, or following industry standards for software security.

174. Progress knew or should have known about the vulnerabilities affecting MOVEit Transfer, and Progress was negligent in developing and maintaining MOVEit Transfer, because:

---

[182] NIST, *CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (CVE-2023-40047) Detail*, Nat'l Vulnerability Database (Aug. 27, 2023), https://nvd.nist.gov/vuln/detail/CVE-2023-40047.

[183] NIST, *CWE-352 Cross-Site Request Forgery (CSRF) (CVE-2023-40048) Detail*, Nat'l Vulnerability Database (Aug. 27, 2023), https://nvd.nist.gov/vuln/detail/CVE-2023-40048.

[184] NIST, *CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (CVE-2022-27665) Detail*, Nat'l Vulnerability Database (Jan. 31, 2024), https://nvd.nist.gov/vuln/detail/CVE-2022-27665.

[185] NIST, *CWE-200 Exposure of Sensitive Information to an Unauthorized Actor (CVE-2023-40049) Detail*, Nat'l Vulnerability Database (Aug. 27, 2023), https://nvd.nist.gov/vuln/detail/CVE-2023-40049.

[186] NIST, *CWE-434 Unrestricted Upload of File with Dangerous Type (CVE-2023-42659) Detail*, Nat'l Vulnerability Database (Nov. 14, 2023), https://nvd.nist.gov/vuln/detail/CVE-2023-42659.

[187] NIST, *CWE-434 Unrestricted Upload of File with Dangerous Type (CVE-2023-40051) Detail*, Nat'l Vulnerability Database (Jan. 26, 2024), https://nvd.nist.gov/vuln/detail/CVE-2023-40051.

[188] NIST, *CWE-305 Authentication Bypass by Primary Weakness (CVE-2024-41403) Detail*, Nat'l Vulnerability Database (Feb. 8, 2024), https://nvd.nist.gov/vuln/detail/CVE-2024-1403.

a. Progress did not adhere to basic, well-known industry standards for software security.

b. Progress did not review and maintain MOVEit Transfer code to ensure it was secure and met industry standards.

c. Progress allowed customers to use outdated versions of MOVEit Transfer software.

d. Progress developed and maintained MOVEit Cloud without the vulnerabilities affecting MOVEit Transfer.

2. Cl0p takes responsibility and ransoms stolen data.

175. Organizations with compromised MOVEit Transfer servers were not immediately contacted with ransom demands when the Data Breach occurred.[189]

176. On June 4, 2023, Microsoft attributed the Data Breach "to Lace Tempest, known for ransomware operations & running the Clop extortion site. The threat actor has used similar vulnerabilities in the past to steal data & extort victims."[190]

177. On June 6, 2023, after the Data Breach was publicized and a patch was rolled out, Cl0p took responsibility for the Data Breach and threatened to post stolen data online unless the compromised organizations paid a ransom.[191]

178. A Cl0p ransom note is reproduced below[192]:

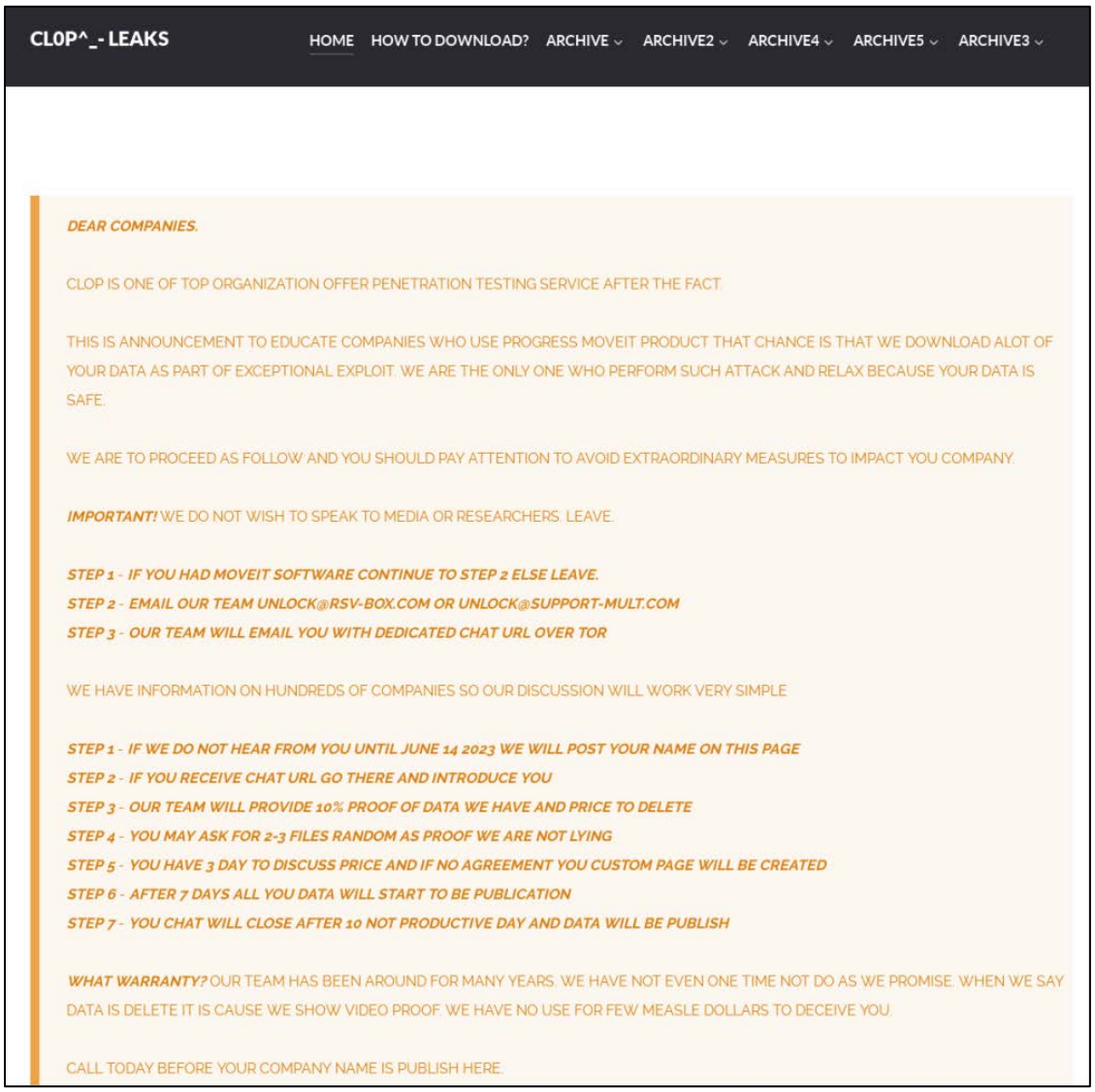
[189] Zaveri, *supra* note 115.

[190] @MsftSecIntel, Twitter (Jun. 4, 2023, 8:55 PM), https://twitter.com/MsftSecIntel/status/1665537730946670595.

[191] Zaveri, *supra* note 115.

[192] Satnam Narang, *CVE-2023-34362: MOVEIt Transfer Critical Zero-Day Vulnerability Exploited in the Wild*, Tenable: Blog (Jun. 2, 2023), https://www.tenable.com/blog/cve-2023-34362-moveit-transfer-critical-zero-day-vulnerability-exploited-in-the-wild.

Figure 6



179. Cl0p threatened to name and publish leaked data of any organizations that did not respond to their ransom demands.[193]

180. The deadline for Cl0p's ransom demands expired on June 14, 2023.[194]

[193] Kim-Mcleod, *supra* note 87.

[194] Kapko, *supra* note 147.

181. On June 14, 2023, Cl0p released a list of 12 organizations that had data compromised in the Data Breach on their dark website >_CLOP^_-LEAKS.[195]

182. Cl0p continued to update this published list and leak terabytes of information, presumably as organizations either rejected or gave into Cl0p's ransom demands.[196]

183. By July 28, 2023, Cl0p had named over 250 organizations on its dark website in relation to the Data Breach.[197]

184. By December 20, 2023, over 2,600 organizations had been named as victims of the Data Breach.[198]

185. Research by Censys found[199]:

- 30.86% of the hosts running MOVEit are in the financial services industry, 15.96% in healthcare, 8.82% in information technology, and 7.56% in government and military.
- 29% of the companies we observed have over 10,000 employees, indicating that this service is used in a variety of large organizations.
- Companies based in the United States account for a significant majority, comprising 69%, of MOVEit hosts.

186. The United States Cybersecurity and Infrastructure Security Agency ("CISA") offered a bounty up to $10 million for information linking Cl0p or other malicious cyber actors targeting United States critical infrastructure to foreign governments.[200]

---

[195] Kim-Mcleod, *supra* note 87.

[196] *Id.*

[197] *Id.*

[198] Bert Kondruss, *MOVEit hack victim list*, Kon Briefing, https://konbriefing.com/en-topics/cyber-attacks-moveit-victim-list.html (last updated Dec. 20, 2023).

[199] *MOVEit: an industry analysis*, Censys: Blogs (June 13, 2023), https://censys.com/moveit-an-industry-analysis/.

[200] @RFJ_USA, Twitter (Jun. 16, 2023), https://twitter.com/RFJ_USA/status/1669740545403437056.

II. The Effects of the Data Breach.

187. The effects of the Data Breach are devastating.

188. Due to the sensitive nature of the information moved using the MOVEit products, the named Plaintiffs and members of the Class have suffered significant exposure and are now at an elevated risk for identity theft and fraud, while many have already experienced significant fraud, identity theft, and other related issues.

189. The kinds of information exposed in the Data Breach provide hackers and cybercriminals a wealth of opportunities for committing additional crimes and harming Plaintiffs and the Class even further.

190. Fraud and identity theft will continue to happen, through the buying, selling, ransoming, and continued exploitation of the personal information, financial information, personal health information, and other sensitive information exposed in this far-reaching Data Breach.

A. The MOVEit software was used to transfer PII and PHI.

191. The MOVEit software was commonly used by healthcare companies, healthcare benefits providers, hospital systems, and other health-related entities, to move Personal Health Information ("PHI").[201]

192. In addition, banking and financial institutions, pension benefit plans, health insurers, colleges and universities, state governments and local municipalities, biotech companies, charter schools, credit unions, emergency services corporations, IT services companies, marketing companies, social service providers, software and technology companies, and many, many more were breached through the MOVEit Transfer and Cloud technologies.[202]

[201] Kondruss, *supra* note 198.

[202] *Id.*

193. In excess of 2,600 different, individual entities were breached via the MOVEit vulnerabilities in the United States alone.[203]

194. Progress's MOVEit technology, both MOVEit Transfer and MOVEit Cloud, were primarily used by Defendants as a secure file-transfer tool.[204]

195. By January 1, 2024, over 93 million individual records had been exposed and the numbers are only growing.

196. The sensitive information moved by these tools was the kind of information each Class member expected would be treated with care and kept confidential, including, but not limited to:

i. Names[205]

ii. Dates of birth[206]

iii. Addresses[207]

iv. Telephone numbers[208]

v. Social Security Numbers[209]

vi. Subscriber/member ID numbers[210]

vii. Driver's License Numbers[211]

---

[203] Kondruss, *supra* note 198.

[204] MOVEit® Transfer Data Sheet, https://webobjects2.cdw.com/is/content/CDW/cdw/on-domain-cdw/brands/progress/progress-moveit-transfer-datasheet0323.pdf (last visited May 20, 2024).

[205] *CMS Notifies Additional Individuals Potentially Impacted by MOVEit Data Breach*, CMS.gov (Nov. 16, 2023), https://www.cms.gov/newsroom/press-releases/cms-notifies-additional-individuals-potentially-impacted-moveit-data-breach.

[206] *Id.*

[207] *Id.*

[208] *Id.*

[209] *Id.*

[210] *Id.*

[211] *Id.*

viii. State Identification Numbers[212]

ix. Policy Numbers[213]

x. Group Numbers[214]

xi. Claim Numbers[215]

xii. Medical history and diagnoses[216]

xiii. Medical bills and claims data[217]

xiv. Financial account numbers[218]

xv. Routing/ABA numbers[219]

xvi. Pension benefit account numbers[220]

xvii. Health insurance ID numbers[221]

xviii. Health insurance claims numbers[222] and

xix. Many other kinds of PII and PHI.

---

[212] *Id.*

[213] *Id.*

[214] *Id.*

[215] *Id.*

[216] *Id.*

[217] *Id.*

[218] Paulina Okunytė, *Kearny Bank admits clients' financial data exposed in MOVEit breach*, cybernews (Nov. 15, 2023), https://cybernews.com/news/kearny-bank-moveit-data-breach/.

[219] Carly Page, *More organizations confirm MOVEit-related breaches as hackers claim to publish stolen data*, Techcrunch (July 6, 2023), https://techcrunch.com/2023/07/06/more-organizations-confirm-moveit-related-breaches-as-hackers-claim-to-publish-stolen-data/.

[220] *CMS Notifies Additional Individuals Potentially Impacted by MOVEit Data Breach*, CMS.gov (Nov. 16, 2023), https://www.cms.gov/newsroom/press-releases/cms-notifies-additional-individuals-potentially-impacted-moveit-data-breach.

[221] *Id.*

[222] *Id.*

197. In each case consolidated in this MDL, the MOVEit server on which Defendants kept Plaintiffs' and Class Members' PII and PHI was compromised, leading to the exposure of the kinds of information identified above.

198. While various Defendants used MOVEit servers to move different kinds of PHI and PII, each and every Defendant used the same MOVEit products to move information of high value and sensitivity.

B. PHI and PII of millions of individuals were exposed to Cl0p and later published to the dark and clear web.

199. Plaintiffs' and Class Members' information was not simply exposed—Cl0p went on to contact organizations in order to extort them by ransoming the stolen information.[223]

200. Prior to the Data Breach, Cl0p was known for using the "double extortion" tactic of stealing and encrypting victim data, refusing to restore victim access, and publishing exfiltrated data on the dark web via the CL0P^_-LEAKS website.[224]

201. In June of 2023, not even a month after the Data Breach was publicized, Cl0p posted the first batch of organizations it claimed to have hacked by exploiting the MOVEit vulnerabilities. The victim list, which was posted to Cl0p's dark web leak site, included U.S.-based financial services organizations 1st Source and First National Bankers Bank; Boston-based investment management firm Putnam Investments; the Netherlands-based Landal Greenparks; and the U.K.-based energy giant Shell.[225]

---

[223] *#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability*, CISA (July 7, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

[224] *Id.*

[225] Carly Page, *Ransomware gang lists first victims of MOVEit mass-hacks, including US banks and universities*, TechCrunch (June 15, 2023), https://techcrunch.com/2023/06/15/moveit-clop-mass-hacks-banks-universities.

202. After gaining access to Defendants' systems, Cl0p contacted senior executives with ransom demands, which often took the form of emails like the one below[226]:

Figure 7

Figure 1: CL0P Ransom Note

Hello, this is the CL0P hacker group. As you may know, we recently carried out a hack, which was reported in the news on site [redacted].

We want to inform you that we have stolen important information from your GoAnywhere MFT resource and have attached a full list of files as evidence.

We deliberately did not disclose your organization and wanted to negotiate with you and your leadership first. If you ignore us, we will sell your information on the black market and publish it on our blog, which receives 30-50 thousand unique visitors per day. You can read about us on [redacted] by searching for CLOP hacker group.

You can contact us using the following contact information:x

unlock@rsv-box[.]com

and

unlock@support-mult[.]com

203. Cl0p also posted warnings on its own leaksite, such as the one below[227]:

[226] *#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability*, CISA (July 7, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

[227] Stefanie Schappert, *Cl0p names first batch of alleged MOVEit victims*, CyberNews (June 15, 2023), https://cybernews.com/news/cl0p-moveit-ransom-attack-victims-names/.

Figure 8

DEAR COMPANIES.

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.

IMPORTANT! WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.

STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.
STEP 2 - EMAIL OUR TEAM UNLOCK@RSV-BOX.COM OR
STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR

WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE.

204. Following the Data Breach, the Federal Bureau of Investigation and the Cybersecurity & Infrastructure Security Agency issued bulletins regarding the MOVEit vulnerabilities and Cl0p's efforts to ransom the PII and PHI of Plaintiffs and Class Members.[228]

205. The FBI and CISA have assembled a comprehensive breakdown of Cl0p's exploitation of the MOVEit SQL injection zero-day vulnerability, which Cl0p used to install a web shell named LEMURLOOT on MOVEit Transfer web applications, along with other malware.[229]

206. The FBI and CISA also provided recommended mitigation strategies, some of which would have assisted in preventing Cl0p from breaking into Defendants' systems.[230]

[228] *Id.*

[229] *Id.*

[230] *Id.*

C. Cl0p's communication with companies exploited by the Data Breach.

207. After exploiting the zero-day SQL vulnerability in the MOVEit software, Cl0p began a campaign of contacting Defendants in this case, setting deadlines designed to extract payments in exchange for promises that the stolen information would not be published. [231]

208. Cl0p's first batch of targets, which included companies like Shell Global, were given until June 14, 2023, to provide ransom payments, or risk having their data exposed on the dark web.[232]

Figure 9

Ramson demand instructions posted on the Cl0p dark leak site

209. While some companies that fell victim to the Data Breach immediately notified their constituencies, others kept mum, preferring to fly below the radar while negotiating with the hackers. This continued until August 15, 2023, when Cl0p published all of the information it had stolen from hundreds of Data Breach targets who refused to pay.[233]

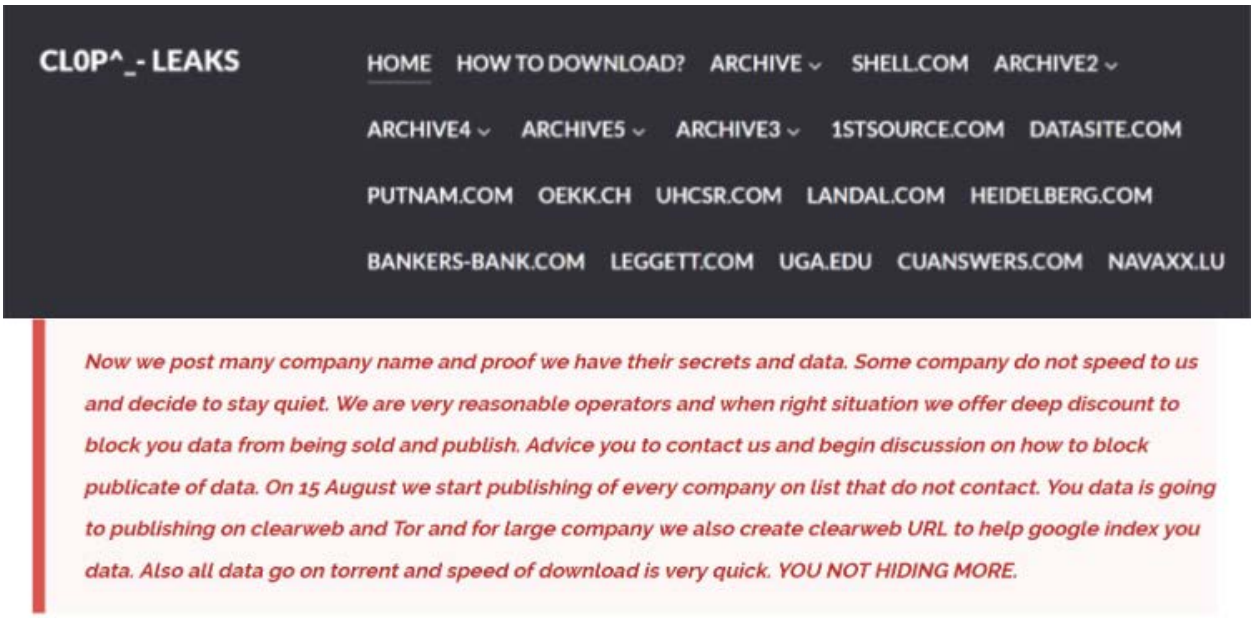
---

[231] *Id.*

[232] *Id.*

[233] *Id.*

Figure 10



210. After apparent negotiation breakdowns, Pricewaterhouse Coopers (PWC) became the first victim to get its own personalized clear web link, at which Cl0p posted Torrent links for all the victim organizations it stole large caches from.[234]

211. Soon after, Cl0p created websites for Aon, EY (Ernst & Young), Kirkland, and TD Ameritrade.[235]

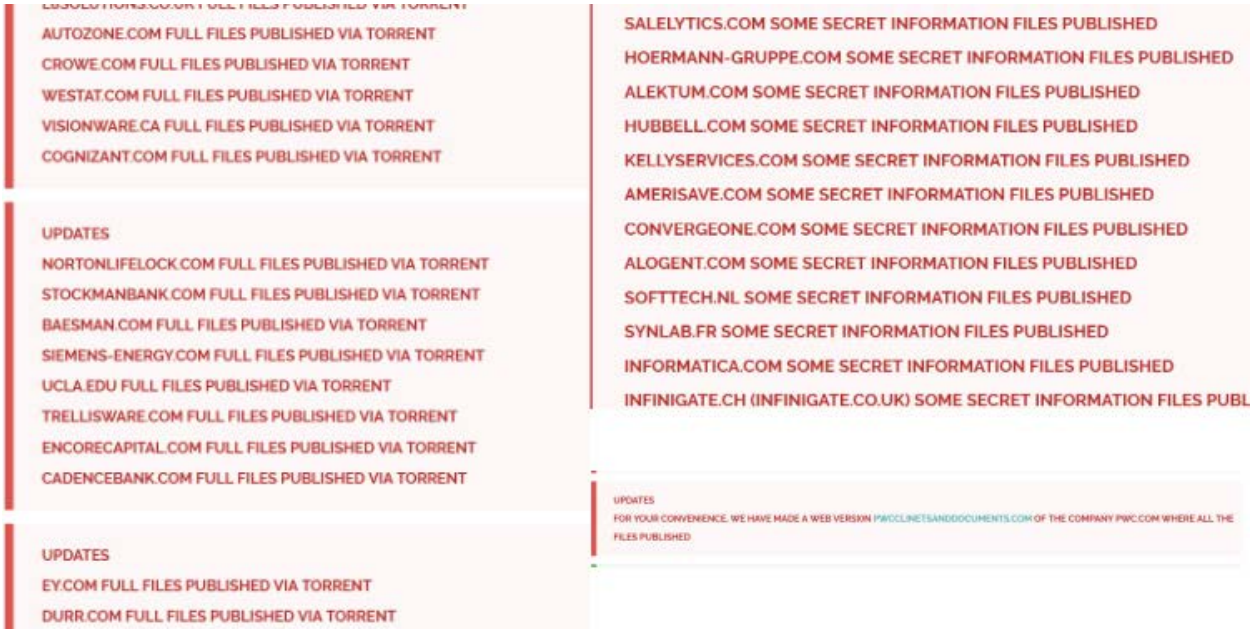
212. Since then, hundreds of caches of PII and PHI stolen from Defendants named in this action were posted on the clear web for open access.[236]

[234] *Id.*

[235] Lawrence Abrams, *Cl0p now leaks data stolen in MOVEit attacks on clearweb sites*, Bleeping Computer (July 23, 2023), https://www.bleepingcomputer.com/news/security/clop-now-leaks-data-stolen-in-moveit-attacks-on-clearweb-sites/.

[236] *Id.*

Figure 11



213. The number of affected organizations has grown exponentially, with over 2,600 different entities within the United States alone.[237]

214. Experienced cybersecurity professionals have acknowledged that the worst may not yet be over: the "broad scope of impact of the MOVEit vulnerability" ensures that more victims will have their PII and PHI exposed on both the dark and clear web, and that no one has a very good idea of when there might be a "light at the end of the tunnel."[238]

D. Cl0p's data destruction promises, like the promises of other cybercriminals, cannot be trusted.

215. The United States government and other law enforcement agencies almost always advise against paying a ransom demand, and that is because cybercriminals cannot be trusted to do what they promise they will do in exchange for a ransom.

[237] Kondruss, *supra* note 198.

[238] Stefanie Schappert, *Cl0p names first batch of alleged MOVEit victims*, CyberNews (June 15, 2023), https://cybernews.com/news/cl0p-moveit-ransom-attack-victims-names/.

216. Indeed, Cl0p is infamous worldwide for their "signature double extortion strategy," which involves the encryption of files on the target's servers, followed by threats to publish the data on the dark or clear web for further exploitation or sale.[239]

217. These tactics are explicitly exploitative: they hinge on extracting monetary concessions from targets based on the dual desires to regain access to their stolen information and contain the impact of the data breach (and potential liability incurred therefrom).

218. Even in cases where Defendants paid a ransom to Cl0p in exchange for decryption and/or promises not to post the stolen data on the clear web, there is no guarantee that the cybercriminals would honor their promises: the hackers could easily have re-copied the stolen data.[240]

219. Indeed, data breach targets that pay ransom demands often cannot substantiate any claimed destruction or return of the data in question.[241]

220. The FBI recognizes the likelihood that cybercriminals will renege on their promises once a ransom is paid, explaining that it "does not advocate paying a ransom, in part because it does not guarantee an organization will regain access to its data."[242]

---

[239] *Id.*

[240] Gary Guthrie, *Paying to delete stolen data doesn't always work out for the victim, new study suggests*, ConsumerAffairs (Nov. 5, 2020), https://www.consumeraffairs.com/news/paying-to-delete-stolen-data-doesnt-always-work-out-for-the-victim-new-study-suggests-110520.html [https://perma.cc/DMV2-JRFP].

[241] *See* Leo Kelion & Joe Tidy, *National Trust Joins Victims of Blackbaud Hack*, BBC News (July 30, 2020), https://www.bbc.com/news/technology-53567699 ("Although Blackbaud has said the cyber-criminals had provided confirmation that the stolen data was destroyed, one expert questioned whether such an assurance could be trusted. 'The hackers would know these people have a propensity to support good causes,' commented Pat Walshe from the consultancy Privacy Matters. This would be valuable information to fraudsters, he added, who could use it to fool victims into thinking they were making further donations when in fact they would be giving away their payment card details.") [https://perma.cc/NC7W-T9LJ]; *Phishing Scams Following Blackbaud Security Breach*, Mich. Dep't Att'y Gen., https://www.michigan.gov/ag/0,4534,7-359-81903_20942-540014--,00.html [https://perma.cc/E6K9-HVZZ].

[242] *High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations*, FBI (Oct. 2, 2019), https://www.ic3.gov/Media/Y2019/PSA191002 [https://perma.cc/VX8P-TW7F].

221. Several media outlets and industry groups have likewise questioned reliance on promises made by cybercriminals.[243]

222. Indeed, many of the Defendants' data breach notifications advised affected individuals to monitor their own credit and financial accounts for suspicious activity

E. Individual victims of cybercriminal data breaches face immediate and significant harm.

223. PII is valuable property. Its value is axiomatic, considering the market value and profitability of "Big Data" to corporations in America. Illustratively, Alphabet Inc., the parent company of Google, reported in its 2020 Annual Report a total annual revenue of $182.5 billion and net income of $40.2 billion.[244] $160.7 billion of this revenue derived from its Google business, which is driven almost exclusively by leveraging the PII it collects about users of its various free products and services.

224. Criminal law also recognizes the value of PII and the serious nature of the theft of PII by imposing prison sentences. This strong deterrence is necessary because cybercriminals extract substantial revenue through the theft and sale of PII. Once a cybercriminal has unlawfully acquired PII, the criminal can demand a ransom or blackmail payment for its destruction, use the PII to commit fraud or identity theft, or sell the PII to other cybercriminals on the black market.

225. Cybercriminals use "ransomware" to make money and harm victims. Ransomware is a widely-known and foreseeable malware threat in which a cybercriminal encrypts a victim's computer such that the computer's owner can no longer access any files or use the computer in

---

[243] *See, e.g.*, Phil Muncaster, *US Data Breach Volumes Plummet 30% in 2020*, Infosecurity Mag. (Oct. 15, 2020), https://www.infosecurity-magazine.com/news/us-data-breach-volumes-plummet-30/ [https://perma.cc/2LYC-XDP6]; Zack Whittaker, *Decrypted: The Major Ransomware Attack You Probably Didn't Hear About*, TechCrunch (Oct. 7, 2020), https://techcrunch.com/2020/10/07/decrypted-blackbaud-ransomware-attack-gets-worse/ [https://perma.cc/R8M4-FMMC].

[244] Alphabet Inc., Annual Report (Form 10-K) at 32 (Feb. 3, 2021), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001652044/000165204421000010/goog-20201231.htm.

any way. The cybercriminal then demands a payment for the decryption key. Ransomware is typically propagated through phishing, spear phishing, or visiting a malicious or compromised website that contains a virus or other malware.

226. Once stolen, PII can be used in many ways. PII can be offered for sale on the dark web, a heavily encrypted part of the Internet that makes it difficult for authorities to detect the location or owners of a website. The dark web is not indexed by normal search engines such as Google and is only accessible using a Tor browser (or similar tool), which aims to conceal users' identities and online activity. The dark web is notorious for hosting marketplaces selling illegal items such as weapons, drugs, and PII. Websites appear and disappear quickly, making it a dynamic environment.

227. The U.S. Government Accountability Office ("GAO") released a report in 2007 regarding data breaches, finding that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[245]

228. The GAO Report explains that "[t]he term 'identity theft' is broad and encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else's name." The GAO Report notes that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[246]

[245] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* ("GAO Report") at 2, GAO (June 2007), https://www.gao.gov/assets/270/262899.pdf [https://perma.cc/GCA5-WYA5].

[246] *Id.*

229. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[247] According to Experian, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to, among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; or use the victim's information in the event of arrest or court action.[248]

230. With access to an individual's PII or PHI, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[249]

[247] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things: "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

[248] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (Sept. 1, 2017), https://www.experian.com/blogs/askexperian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-youprotect-yourself/.

[249] *Id.*

231. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[250]

232. Theft of SSNs creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new SSN, a breach victim has to demonstrate ongoing harm from misuse of their SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

233. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (*e.g.*, name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating: "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[251]

F. It is reasonable for individual victims of cybercriminal data breaches to take actions to mitigate their risk of harm.

234. Cybercriminals can and do use the PII and PHI that Defendants were entrusted to safeguard to perpetrate financial crimes that harm Plaintiffs and the Class.

235. In addition to all the other immediate consequences of the Data Breach, Plaintiffs and Class Members face a substantially increased risk of identity theft and fraud.

236. The Federal Trade Commission ("FTC") recommends that identity theft victims take several steps to protect their personal health and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and to consider an extended

[250] *Id.*

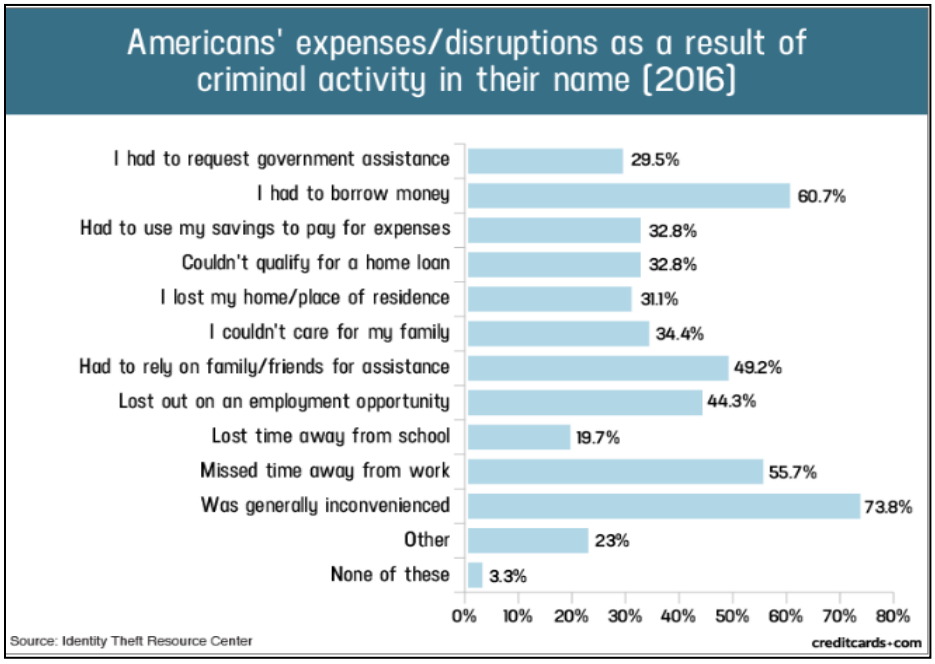
[251] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, Identity Theft Resource Center (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/.

fraud alert that lasts for seven years if identity theft occurs), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[252]

237. Cybercriminals use stolen PII such as SSNs for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

238. A study by the Identity Theft Resource Center ("ITRC") shows the multitude of harms caused by fraudulent use of personal and financial information[253]:

Figure 12



239. As set forth above, 96.7% of study subjects experienced costs or other harms from the criminal activity.[254] As illustrated in the above graphic, this includes devastating results such

[252] Identity Theft Recovery Steps, FTC, https://www.identitytheft.gov/Steps (last visited Mar. 23, 2021). Indeed, the FTC takes data breaches seriously, and has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information can constitute an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

[253] Jason Steele, Credit Card and ID Theft Statistics, Creditcards.com (updated Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

[254] *Id.*

as: "I lost my home/place of residence" and "I couldn't care for my family." Moreover, the harms of identity theft are not limited to the affected individual and may adversely impact other associated persons and support systems, including government assistance programs. In the ITRC study, nearly one third of survey respondents had to request government assistance because of identity theft, such as welfare, EBT, food stamps, or similar support systems.[255] The ITRC study concludes that "identity theft victimization has an extreme and adverse effect on each individual as well as all of the support systems and people associated with the individual."[256]

240. PII is a valuable property right.[257] Its value is axiomatic, considering the value of Big Data in corporate America as well as the consequences of cyber thefts resulting in heavy prison sentences. This obvious risk to reward analysis illustrates that Private Information has considerable market value that is diminished when it is compromised.

241. There may also be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the GAO Report: "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[258]

---

[255] *Id.*

[256] *Id.*

[257] *See, e.g.*, John T. Soma et al., Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *1 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.").

[258] GAO Report at 29, *supra* note 245.

242. PII is such an inherently valuable commodity to identity thieves that, once it is compromised, criminals often trade the information on the cyber black-market for years.

243. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[259]

244. Medical identity theft "is also more difficult to detect, taking almost twice as long as normal identity theft."[260] In warning consumers of the dangers of medical identity theft, the FTC states that an identity thief may use PII and PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[261] The FTC also warns, "If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[262]

245. A report published by the World Privacy Forum[263] and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

a. Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.

---

[259] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

[260] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), https://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.

[261] *See* FBI, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (Apr. 8, 2014) at 14, https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems cyber-intrusions.pdf.

[262] *See* FTC, *What to Know About Medical Identity Theft*, FTC Consumer Information, https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited May 20, 2025).

[263] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017) at 24, https://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.

b. Significant bills for medical goods and services not sought or received.

c. Issues with insurance, co-pays, and insurance caps.

d. Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.

e. Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

f. As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgages or other loans and may experience other financial impacts.

g. Phantom medical debt collection based on medical billing or other identity information.

h. Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.

246. Furthermore, data breaches that expose any personal data, and in particular non-public data of any kind (*e.g.*, donation history or hospital records), directly and materially increase the chance that a potential victim is targeted by a spear phishing attack in the future, and spear phishing results in a high rate of identity theft, fraud, and extortion.[264]

247. The United States Court of Appeals for the First Circuit has recognized that it is not necessary for a victim of a data breach to have their identity stolen, or to suffer actual fraud, for it to be reasonable for a data breach victim to take steps to protect themselves.[265]

---

[264] *See* Kelion & Tidy, *supra* note 241 (concluding that personal information such as "names, titles, telephone numbers, email addresses, mailing addresses, dates of birth, and, more importantly, donor information such as donation dates, donation amounts, giving capacity, philanthropic interests, and other donor profile information . . . . in the hands of fraudsters, [makes consumers] particularly susceptible to spear phishing—a fraudulent email to specific targets while purporting to be a trusted sender, with the aim of convincing victims to hand over information or money or infecting devices with malware").

[265] *Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365, 371 (1st Cir. 2023). In *Webb*, the First Circuit concluded that "plausible allegations of actual misuse [of PII] . . . state a concrete injury under Article III." *Webb*, 72 F.4th at 373. The First Circuit is in agreement with other circuits that have encountered the same question. *See, e.g.*, *In re Equifax Inc. Customer Data Sec. Breach Litig.*, 999 F.3d 1247, 1262 (11th Cir. 2021); *Attias v. CareFirst, Inc.*, 865 F.3d 620, 627 (D.C. Cir. 2017); *In re Marriott, Int'l, Inc. Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 459

248. As the United States Court of Appeals for the Seventh Circuit aptly observed almost a decade ago: "the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."[266]

249. This remains true, ten years later. The intent of hackers (such as Cl0p) is clear when they hack systems, such as the Defendants': they are attempting to access consumers' PHI and PII for the purpose of ransoming it back, and/or selling it for a profit.

250. There may be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. On average, it takes approximately three months for a consumer to discover their identity has been stolen and used and it takes some individuals up to three years to learn that information.[267]

251. In addition, there is a strong probability that much of the information stolen in the Data Breach has not yet been made available on the black market in a coherent, organized fashion,[268] meaning Plaintiffs and Class Members will remain at an increased risk of fraud and identity theft for many years into the future. Indeed, some Class Members are in very early stages of their lives—in their twenties and thirties. Thus, as the respective Data Breach Notices advise, customers, including Plaintiffs and Class Members, must vigilantly monitor their financial accounts for many years to come.

(D. Md. 2020); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 690 (7th Cir. 2015) ("customers should not have to wait until hackers commit identity theft or credit-card fraud" in order for their mitigation efforts to be reasonable and compensable).

[266] *Remijas*, 794 F.3d at 693.

[267] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

[268] Schappert, *supra* note 227 (describing certain data stolen from MOVEit customers and put on the clear web by Cl0p as "a challenge for us to download," and noting that the data is "unstructured.").

G. Defendants' actions have been insufficient to protect consumers or compensate victims.

252. The Defendants in this action did not take sufficient steps to protect their customers, and have not done nearly enough to compensate the victims of the Data Breach, who will suffer real harm for years to come.

253. As an initial matter, Defendants did not take the most basic steps to ensure network security.

254. The industries that Defendants serve have seen a substantial increase in cyberattacks and data breaches since as early as 2016.[269]

255. Indeed, cyberattacks have become so notorious that the FBI and Secret Service issued a warning in 2019 to potential targets so they were aware of, and prepared for, a potential attack.[270]

256. Cybersecurity efforts have developed apace to provide an answer to these rising attacks and multiplying attack vectors. In 2019, both Microsoft and Google publicly reported that using multi-factor authentication ("MFA") blocks more than 99% of automated hacks, including most ransomware attacks that occur because of unauthorized account access. Likewise, the reputable SANS Software Security Institute issued a paper stating: "[t]ime to implement multi-factor authentication!"[271] An example of MFA implementation is receiving a text with a code when you input your username and password into a website; even if a cybercriminal knew your username

[269] *Id.*

[270] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, Law360 (Nov. 18, 2019), https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware [https://perma.cc/Z6GF-777F].

[271] Matt Bromiley, *Bye Bye Passwords: New Ways to Authenticate* at 3, SANS Software Security Inst. (July 2019), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3y9UJ.

and password, the cybercriminal would not be able to see the code on your phone and would thus be blocked from accessing your online account.

257. In this regard, implementing MFA "can block over 99.9 percent of account compromise attacks."[272]

258. The FBI concurs, listing "applying two-factor authentication wherever possible" as a best practice to defend against ransomware attacks.[273]

259. Cybersecurity experts agree: "MOVEit should be behind technologies that provide access to only those who need it via tools such as Zero Trust (*e.g.*, access gateways secured by MFA) or simple allowlists and blocklists."[274]

260. Experts further recommend: "If you run MOVEit within your organization, ensure that the database runs as a specific user that can only interact with MOVEit and not as a superuser with broader access. The exploit utilizes SQL injection to allow attackers to manipulate server databases and execute arbitrary code, resulting in data exfiltration. Because this breach is an SQL injection leading to remote code execution (RCE), the adversary only gains initial access to the database server and user."[275]

261. Defendants also could have employed (either internally or through third parties) competent professionals to act as 24/7 "eyes on glass." Providers of managed security services,

---

[272] *What Is Multi-Factor Authentication (MFA)?*, Consensus Techs. (Sept. 16, 2020), https://www.concensus.com/what-is-multi-factor-authentication.

[273] *Ransomware Victims Urged to Report Infections to Federal Law Enforcement*, FBI (Sept. 15, 2016), https://www.ic3.gov/Media/Y2016/PSA160915.

[274] Steve Cobb, *Three Steps to Prevent a Cybersecurity Breach from MOVEit Exploit*, SecurityScorecard (June 7, 2023), https://securityscorecard.com/blog/three-steps-to-prevent-a-cybersecurity-breach-from-moveit-exploit-securityscorecards-investigation-into-zellis-reach-uncovers-2500-exposed-moveit-servers-across-790-organizations/.

[275] *Id.*

also referred to as "managed detection and response" ("MDR") employ a sophisticated series of artificial and human intelligence to monitor for signs that a breach is underway.

262. The MOVEit SQL injection vulnerability was exploited by Cl0p in order to execute a series of commands that ultimately resulted in the exfiltration of data. Either on their own or through the use of a qualified third-party vendor, Defendants could and should have been monitoring their own systems and repositories for indications of compromise ("IOCs,"), which would have included external injection of SQL code by unauthorized users. Companies have an obligation to monitor their systems for the execution of unauthorized code. If Defendants had appropriate monitoring in place, they could have detected, and prevented this attack.

263. Indeed, companies who were using appropriate managed security detected the MOVEit vulnerability as early as May 27, 2023, and were able to take steps to prevent the large-scale exfiltration of consumers' sensitive information. For instance, on May 27, 2023, researchers for Akamai (a cybersecurity company) fended off an attempt by Cl0p to use the MOVEit exploitation against one of Akamai's financial customers, "an attack that was blocked by the Akamai Adaptive Security Engine."[276]

264. There were services available for Defendants to detect the Data Breach and prevent large scale exfiltration of the PII and PHI entrusted to them, but Defendants simply failed to appropriately implement these services.

265. Furthermore, it does not take cybersecurity expertise to know Defendants should not have maintained—or allowed the maintenance of—millions of consumers' PII and PHI on MOVEit software, where it was a sitting duck waiting for a cyberattack such as the Data Breach.

[276] Akamai Security Intelligence Group, *MOVEit SQLi Zero-Day (CVE-2023-34362) Exploited by CL0P Ransomware Group*, Akamai Blog (June 8, 2023), https://www.akamai.com/blog/security-research/moveit-sqli-zero-day-exploit-clop-ransomware.

266. There were plenty of technologies and processes readily available that Defendants could have utilized to prevent the Data Breach. Defendants failed to do so.

267. The problem caused by Defendants' unwillingness to take proper data security precautions will only get worse: a study published in May 2022 by the International Data Corporation projects that the amount of new data created, captured, replicated, and consumed is expected to double in size by 2026.[277]

268. With an increase in data creation comes a heightened risk of data breaches and bad actors gaining access to personal information. One result of data breaches, identity theft, poses a serious threat to consumers engaging in online transactions and across a host of digital platforms. Both state and federal laws and regulations impose standards of reasonable security measures for businesses so consumers can, in turn, feel safe sharing their Private Information in the marketplace.

269. Data privacy is important to the public: according to a survey conducted by cyber-security company FireEye, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[278]

270. Data breaches are not an unpreventable occurrence. In the Data Breach and Encryption Handbook, Lucy Thompson wrote, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of

[277] *See* John Rydning, *Worldwide IDC Global DataSphere Forecast, 2022–2026: Enterprise Organizations Driving Most of the Data Growth*, IDC (Nov. 2022), https://www.idc.com/getdoc.jsp?containerId=US49759222.

[278] FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 11, 2016), https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited Mar. 5, 2021).

appropriate security solutions." She continued, "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[279]

271. The Defendants in these consolidated cases knew there were steps they could take to secure their systems and protect the PII and PHI of their customers; they simply chose not to take them.

H. Damages can compensate victims for the harm caused by the breach.

272. To the injury of failing to protect their systems with readily available technology services designed to curtail or prevent data breaches like the MOVEit breach, resulting in the exposure of Plaintiffs' and Class Members' PII and PHI, Defendants have added the insult of refusing to provide even paltry compensation.

273. While several Defendants have offered victims of the Data Breach credit monitoring services, these services alone are not enough: a year or two of credit monitoring will not un-ring the bell of the release of the PII and PHI of the Plaintiffs and Class Members, which will circulate through the various levels of the internet (clear, dark, and deep) for years and years, if not in perpetuity. Particularly considering the fact that Social Security numbers were exposed in the Data Breach, Data Breach victims will need to monitor their credit and accounts for years and years to come—and these services are typically accounted for in settlements and judgments involving data breaches.[280]

[279] Lucy L. Thomson, Data Breach and Encryption Handbook (Am. Bar Assoc. 2011).

[280] For instance, in July 2019, the CFPB, FTC and States announced a settlement with Equifax over the 2017 Equifax data breach, which included up to ten years of credit monitoring and identity restoration services. *See CFPB, FTC and States Announce Settlement with Equifax Over 2017 Data Breach*, CFPB (July 22, 2019), https://www.consumerfinance.gov/about-us/newsroom/cfpb-ftc-states-announce-settlement-with-equifax-over-2017-data-breach/.

274. The PII and PHI exposed in the Data Breach has real value, as explained above. Plaintiffs and the Class have therefore been deprived of their rights to the control of that property and have lost the value they might otherwise have incurred from that data.[281]

275. Plaintiffs and the Class have spent significant time, and will spend more, monitoring their accounts, changing login credentials, and recovering from the inevitable fraud and identity theft which will occur, which deserves to be compensated: Defendants have not made apportionment for this very real injury.[282]

276. Similarly, Defendants have offered no compensation for the aggravation, agitation, anxiety, and emotional distress that Plaintiffs and the Class have suffered, and will continue to suffer, as a result of the Data Breach: the knowledge that their information is out in the open, available for sale and exploitation at any time in the future is a real harm that also deserves compensation.

277. Plaintiffs and members of the Class were also deprived of the benefit of their bargain when they interacted with Defendants: each Defendant had a duty to take reasonable steps to protect the PII and PHI of its customers. This duty was inherent in the relationships between Plaintiffs and Class Members and Defendants, whether through express contractual terms, implied contractual terms, or statutory or implied duties of good faith and fair dealing.

278. Defendants have not taken sufficient steps or even attempted to make their customers, the real victims in this Data Breach, whole. Defendants have failed their duty to protect

[281] Ravi Sen, *Here's how much your personal information is worth to cybercriminals – and what they do with it*, PBS, May 14, 2021 https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it.

[282] Time spent monitoring accounts is another common and cognizable, compensated harm in data breach cases. *See* Equifax Data Breach Settlement FAQ, FTC, Dec. 2022, https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement.

Plaintiffs' and Class Members' PHI and PII and have failed in their duty to help these consumers protect themselves in the future.

I. This case demonstrates that the risk of harm and class member injuries are not hypothetical.

279. Plaintiffs who have filed suit in this multidistrict litigation have suffered injuries in a number of ways, including:

a. Loss of benefit of their bargain, for individuals who provided compensation to entities to safely transfer and store their data with one of the Defendants or Defendants' vendors;

b. Loss of value of their personal information, in that it has been misused for purposes to which they did not consent, and they have not been properly compensated for this misuse;

c. Actual or attempted fraud, misuse, or identity theft caused by the Data Breach, including, but not limited to, their information being published to the clear, deep, and dark web; as well as

d. Time and expenses that were reasonably spent to mitigate the impact of the breach.

280. Several Plaintiffs have already experienced actual or attempted fraud, which is reasonably related to the Data Breach, which demonstrates that the Data Breach has put them at immediate risk for additional harm.

281. The harm already suffered by Plaintiffs demonstrates that the risk of harm is ongoing.

III. Preventing the Data Breach.

282. Progress could have prevented the Data Breach by following industry standards for secure software development and maintenance.[283]

[283] *MOVEit Data Breach: Summary and How to Prevent SQL Injection Attacks*, *supra* note 283.

283. The remaining Defendants could also have prevented or mitigated against the risk of the Data Breach through implementation of security-standard data management, software review, data mapping, risk management, employment of zero-trust policies, and diligence concerning Progress's software.

A. Secure software development.

284. Progress could have prevented the Data Breach by following secure software development practices by default, rather than seeking to maintain and patch outdated software with critical security vulnerabilities for decades.[284]

285. Secure software development "focuses on identifying and mitigating security risks from the early stages of development to the deployment and maintenance phases."[285]

286. Secure software development includes[286]:

a. Threat modeling

b. Secure coding practices

c. Secure code review and testing

d. Security training and awareness

e. Ongoing maintenance and updates

287. Following secure software development practices from the beginning of development through release and maintenance of the software is an industry standard and best practice because it avoids the potential for overlooking a security vulnerability in outdated code.[287]

[284] *Id.*

[285] *Id.*

[286] *Id.*

[287] *Id.*

288. Progress and its predecessors failed to follow secure software development practices from the initial development of MOVEit Transfer because they included code with critical security vulnerabilities—including code susceptible to SQL injection—and then overlooked or did not attempt to discover such vulnerabilities when maintaining the software.[288]

B. Monitoring potential security risks.

289. Progress could have prevented the Data Breach by monitoring potential security risks identified by the software development industry.[289]

290. The software development industry publishes numerous resources for developers to learn about old, new, and emerging areas of potential vulnerability, such as the OWASP Top 10, which lists the 10 most serious potential security vulnerabilities in the industry today.[290]

291. SQL injection is the third most critical security risk on the OWASP Top 10.[291]

292. SQL injection is frequently discussed as a widespread and easy to prevent vulnerability.[292]

293. Vulnerable and outdated components are the sixth most critical security risk on the OWASP Top 10.[293]

294. The BinaryFormatter.Deserialize remote code execution vulnerability has been documented and easy to prevent since at least 2017.[294]

---

[288] *Id.*

[289] *Id.*

[290] *Id.*

[291] *OWASP Top 10*, *supra* note 64.

[292] Yasar, *supra* note 40.

[293] *OWASP Top 10*, *supra* note 64.

[294] *BinaryFormatter serialization methods are obsolete and prohibited in ASP.NET apps*, *supra* note 77; *A8:2017-Insecure Deserialization*, *supra* note 80; *OWASP Top 10*, *supra* note 64; pwntester, *supra* note 82.

295. Monitoring developments in software security from industry resources is a best practice because it flags old, new, and emerging areas of potential vulnerability.[295]

296. Progress failed to monitor potential security risks because they included code in MOVEit Transfer with critical security vulnerabilities—such as SQL injection and deserialization—that are frequently identified by the software development industry as critical potential vulnerabilities.[296]

C. Sanitizing and validating user input.

297. Progress could have prevented the Data Breach by designing MOVEit Transfer to sanitize and validate user input, rather than "trusting" user input as safe.[297]

298. Sanitizing and validating user input is an industry standard and best practice because it ensures that data meets the criteria expected by the software, whether authorized or malicious, and stops potential sources of malicious code from reaching the database.[298]

299. Progress failed to sanitize and validate user input because they allowed MOVEit Transfer to pass user input directly to the SQL engine, such that malicious code within user input could be executed by the server.[299]

D. Static code analysis.

300. Progress could have prevented the Data Breach by strictly analyzing their code for potential security vulnerabilities.[300]

---

[295] *MOVEit Data Breach: Summary and How to Prevent SQL Injection Attacks*, *supra* note 283.

[296] *Id.*

[297] *Id.*

[298] *Id.*

[299] *Id.*

[300] *Id.*

301. Static code analysis is an industry standard and best practice because it ensures that code is written in a manner that not only provides the expected output, but prevents unexpected or even harmful outputs, such as SQL injection and remote code execution.[301]

302. Analysis of MOVEit Transfer code by a competent developer would have revealed glaring vulnerabilities that could have been removed before the Data Breach, including:

a. Passing unsanitized, unvalidated user input into SQL queries[302]

b. Failing to use parameterized statements to prevent SQL injection[303]

c. Using the BinaryFormatter.Deserialize function[304]

303. Third-party tools can analyze code for vulnerabilities that may be easy or hard to identify, including SQL injection and deprecated functions.[305]

304. Progress failed to analyze the MOVEit Transfer code for potential security vulnerabilities, instead blindly relying on outdated, poorly written code that performed as Progress expected under controlled conditions.[306]

E. Vulnerability testing.

305. Progress could have prevented the Data Breach by testing its code for potential security vulnerabilities, rather than simply using code that performed correctly under controlled conditions.[307]

---

[301] *Id.*

[302] Yasar, *supra* note 40.

[303] *Id.*

[304] *BinaryFormatter serialization methods are obsolete and prohibited in ASP.NET apps*, *supra* note 77; *A8:2017-Insecure Deserialization*, *supra* note 73; *OWASP Top 10*, *supra* note 64; pwntester, *supra* note 82.

[305] Dave Wichers et al., *Source Code Analysis Tools*, OWASP, https://owasp.org/www-community/Source_Code_Analysis_Tools (last visited Apr. 26, 2024).

[306] *MOVEit Data Breach: Summary and How to Prevent SQL Injection Attacks*, *supra* note 283.

[307] *Id.*

306. Vulnerability testing is an industry standard and best practice because it subjects code to scrutiny and unexpected user input so that critical flaws can be discovered.[308]

307. Vulnerability testing involves subjecting software to extreme conditions that may be unexpected in the real world—such as sending improperly formatted requests to incorrect ports—in order to understand how the software reacts and whether any conditions can cause the software to fail or become insecure.[309]

308. Third-party tools can perform vulnerability testing by engaging in a range of interactions with the software while measuring performance.[310]

309. Progress failed to analyze the MOVEit Transfer code for potential security vulnerabilities, instead blindly relying on outdated, poorly written code that performed as Progress expected under controlled conditions.[311]

F. External penetration testing.

310. Progress could have prevented the Data Breach by subjecting their software to penetration testing by a third-party security firm.[312]

311. Penetration testing is an industry standard and best practice because it subjects code to concerted attack scenarios that test its ability to withstand a data breach.[313]

---

[308] *Id.*

[309] Vitaly Unic, *Vulnerability Testing: Methods, Tools, and 10 Best Practices*, Bright (May 15, 2023), https://brightsec.com/blog/vulnerability-testing-methods-tools-and-10-best-practices/.

[310] *Id.*

[311] *MOVEit Data Breach: Summary and How to Prevent SQL Injection Attacks*, *supra* note 283.

[312] *Id.*

[313] *Id.*

312. Penetration testing is performed by third-party security firms with expertise in hacking software, whereby the firm attempts to compromise the software using a variety of tactics to test its resilience to an organized attack.[314]

313. Progress failed to perform penetration testing on MOVEit Transfer, allowing the software to be used without any understanding of its ability to withstand an attempted data breach.[315]

IV. Progress's culpability for Plaintiffs' and Class Members' losses.

A. Progress knew its software was being used to transfer sensitive information.

314. Progress knows and intends for MOVEit to be used by its customers to transfer and receive highly sensitive Private Information.

315. Progress represents itself as "a global supplier of products and services for business applications" that "develops, markets and distributes application development, deployment, integration and management software to business, industry and governments worldwide."[316]

316. Progress claims "to deliver superior software products and services that empower [its] partners and customers to dramatically improve their development, deployment, integration and management of quality applications worldwide.[317]

317. Progress specifically advertises and markets MOVEit to potential customers in the following industries: (a) banking and financial services; (b) educational services; (c) healthcare;

---

[314] *Id.*

[315] *Id.*

[316] Progress, SEC Form 10-K (2003), https://www.sec.gov/Archives/edgar/data/876167/000095013503001256/b45503pse10vk.htm.

[317] *Id.*

(d) insurance; (e) manufacturing; (f) public sector; (g) retail; and (h) the United States Federal Government.[318] Indeed, Progress knows that:

a. "Banking, Financial Services and Insurance companies around the globe depend on MOVEit for secure, scalable and compliant file transfer."[319]

b. MOVEit is used by "educational institutions of all sizes."[320]

c. "Healthcare organizations around the globe depend on Progress MOVEit managed file transfer to enable more secure, scalable, reliable file sharing to power patient care, business services and help maintain compliance.[321]

d. "MOVEit is the leading secure managed file transfer software that enables online retailers to exchange very sensitive information such as payment information, inventory reports, and other sensitive data quickly and securely across multiple stores and offices."[322]

e. "MOVEit managed file transfer is the leading [managed file transfer] application for federal government file sharing and file security compliance."[323]

318. Progress is aware and understands that its customers' businesses depend on "transferring mission critical, sensitive data securely and reliably."[324]

319. Progress markets, advertises, guarantees, and warrants to all its customers that the MOVEit Transfer software will keep Private Information safe and secure from unauthorized access.

---

[318] *MOVEit –Managed File Transfer Software – Use Cases, By Industry*, Progress, https://www.progress.com/moveit (last visited Apr. 23, 2024).

[319] *MOVEit –Managed File Transfer for Banking and Financial Services*, Progress, https://www.progress.com/moveit/banking-and-finance (last visited Apr. 23, 2024).

[320] *MOVEit –Managed File Transfer for Education*, Progress, https://www.progress.com/moveit/education (last visited Apr. 23, 2024).

[321] *MOVEit –Managed File Transfer for Healthcare*, Progress, https://www.progress.com/moveit/healthcare (last visited Apr. 23, 2024).

[322] *MOVEit – Secure File Transfer for Retail*, Progress, https://www.progress.com/moveit/retail (last visited Apr. 23, 2024).

[323] *MOVEit – FIPS Validated File Transfer Products*, Progress, https://www.progress.com/moveit/government-us-federal-government (last visited Apr. 23, 2024).

[324] *Managed File Transfer Software*, Progress, https://www.progress.com/moveit (last visited May 20, 2024).

320. Progress promises that MOVEit will "provide a *secure environment* for your most sensitive files, while easily ensuring the reliability of core business processes."[325]

321. According to Progress: "In a world built on distributed work and collaboration, securing sensitive files is essential. Progress offers file transfer solutions that secure and encrypt your sensitive files, offer new levels of operational efficiency and meet the compliance standards that matter most to your organization."[326]

322. Progress holds itself out publicly as a trustworthy industry leader worldwide by advertising that customers should "trust Progress for innovation and results" and boasting that "top 10 tech companies rely on Progress," "the 30 largest companies in the world trust Progress," and "70% of Fortune 500 companies trust Progress."[327]

323. In marketing the MOVEit Transfer software to businesses in a broad range of industries, Progress warrants and promises to customers that MOVEit "makes it easy to choose the exact capabilities that match your organization's specific needs."[328]

324. Progress promises its clients in the educational services sector that "MOVEit managed file transfer provides easy, secure, automated and compliant movement of PII and other highly sensitive files."[329]

---

[325] *Id.* (emphasis added).

[326] *Secure File Transfer – Essential Security for Your Most Important Files*, Progress, https://www.progress.com/file-transfer (last visited May 20, 2024).

[327] *Trust Progress for Innovation and Results*, Progress, https://www.progress.com/ (last visited May 20, 2024).

[328] *MOVEit –Managed File Transfer Software*, Progress, https://www.progress.com/moveit (last visited Apr. 23, 2024).

[329] *MOVEit –Managed File Transfer for Education*, Progress, https://www.progress.com/moveit/education (last visited Apr. 23, 2024).

325. Progress promises its customers in the healthcare industry that it knows "the business of healthcare depends on the reliable, secure and compliant transfer of Protected Health Information (PHI)."

326. Progress intended for its customers to rely on its promises and representations that MOVEit would keep Private Information secure from unauthorized access and ensure its customers' compliance with industry standards and regulatory requirements related to data security.

327. Progress further warrants that MOVEit complies with applicable data security laws and regulations, marketing MOVEit as a tool that will "[e]nsure regulatory compliance in the transfer of PII and Financial Data."[330]

328. Progress claims "MOVEit enables your organization to meet strict cybersecurity compliance standards such as PCI-DSS, HIPAA, GDPR, SOC2, and more."[331]

329. Progress warns its clients and potential clients that "[i]ncreasingly strict data protection regulations mandate that networks, user access, databases and business processes are secured to protect financial data and customers' Personally Identifiable Information (PII)."[332]

330. Accordingly, Progress represented that MOVEit would ensure regulatory compliance for customers.

[330] *See, e.g.*, *MOVEit –Managed File Transfer for Education*, Progress, https://www.progress.com/moveit/education (last visited Apr. 23, 2024).

[331] *MOVEit –Managed File Transfer Software*, Progress, https://www.progress.com/moveit (last visited Apr. 23, 2024).

[332] *MOVEit –Managed File Transfer for Education*, Progress, https://www.progress.com/moveit/education (last visited Apr. 23, 2024).

331. Progress promises its customers in the financial industry that MOVEit will "help[] your organization meet cybersecurity compliance standards such as PCI-DSS, HIPAA, GDPR, SOC2 and more."[333]

332. Progress also recognizes that "[e]ducational institutions need to protect the personally identifiable information (PII) of students, employees, and other stakeholders every day. In addition, valuable intellectual property, health records and other sensitive information require security, visibility, and control that is in line with leading cybersecurity standards such as HIPAA, GDPR, PCI-DSS, and others."[334]

333. Progress promises its clients in the educational services industry that "[t]he MOVEit suite of Secure Managed File Transfer products assures encryption of external data transfers, delivery to the intended recipient and detailed audit logs. MOVEit provides the security features and flexible deployments that enable you to meet SOX, GLB, PCI and GDPR data protection requirements."[335]

334. Progress likewise promises its clients in the healthcare industry that "MOVEit provides the features and deployment flexibility required to help healthcare agencies comply with HIPAA, PCI-DSS, GDPR and other leading cybersecurity standards."[336]

335. Progress warranted that MOVEit would provide protection against the exact dangers and resulting damages it instead exposed and inflicted upon its customers and Plaintiffs.

---

[333] *MOVEit –Managed File Transfer Software*, Progress, https://www.progress.com/moveit (last visited Apr. 23, 2024).

[334] *MOVEit –Managed File Transfer for Education*, Progress, https://www.progress.com/moveit/education (last visited Apr. 23, 2024).

[335] *MOVEit –Managed File Transfer for Education*, Progress, https://www.progress.com/moveit/education (last visited Apr. 23, 2024).

[336] *MOVEit –Managed File Transfer for Healthcare*, Progress, https://www.progress.com/moveit/healthcare (last visited Apr. 23, 2024).

336. Progress knew or should have known that the statements and promises it made regarding MOVEit were false and misleading, based on its subpar database development, security procedures, and controls.

B. Progress knew of the risks of data breaches and the damage a breach of its software could create.

337. Progress knows that "[d]ata in motion is data at risk and particular attention must be paid to the security and compliance of [its customers'] external file transfer process."[337]

338. A data breach is a foreseeable consequence of failing to adequately design and maintain a file transfer application like MOVEit.

339. Indeed, such consequences have been seen in similar widely publicized breaches involving file transfer solutions like MOVEit—including Accellion FTA and Fortra GoAnywhere MFT.

340. In the Accellion, Inc. breach, over 100 companies, organizations, universities, and government offices were subject to ransomware attacks as a result of vulnerabilities in its system.

341. The highly public nature of the Accellion, Inc. breach and similar breaches placed Progress on notice of the foreseeable consequences of its failure to adequately design and maintain its MOVEit applications.

342. Moreover, the fact that CVE-2023-34362 existed for at least two years prior to the Data Breach indicates that Progress, as the developer of MOVEit, knew or should have known of the vulnerability using reasonably diligent efforts.

343. Despite adequate notice of the risks associated with its failure to adequately design, maintain, and proactively test the MOVEit application, Progress failed to ensure the security of its

[337] *MOVEit –Managed File Transfer for Banking and Financial Services*, Progress, https://www.progress.com/moveit/banking-and-finance (last visited Apr. 23, 2024).

platform and ultimately the security of the highly sensitive and confidential Private Information transferred by its customers' using MOVEit.

344. Progress failed to expend the necessary funds to ensure the product it designed, marketed, sold, distributed, and maintained was safe and secure.

345. As a result, the MOVEit Data Breach created astounding financial repercussions for Progress's customers as well as the many entities and individuals who entrusted Progress's customers with their highly sensitive and confidential Private Information and relied on Progress and Progress's customers to protect and secure that information from unauthorized disclosure

C. Progress had an obligation to identify and remediate any vulnerabilities in the MOVEit software.

346. By marketing and advertising MOVEit as a solution for secure transfer and storage of highly sensitive Private Information, Progress assumed legal and equitable duties and knew or should have known it was responsible for:

a. adequately designing, maintaining, and updating its software;

b. promptly detecting, remediating, and notifying its customers of any critical vulnerabilities in its software code;

c. ensuring compliance with industry standards related to data security;

d. ensuring compliance with regulatory requirements related to data security;

e. protecting and securing the Private Information contained in its customers' files from unauthorized disclosure; and

f. providing adequate notice to customers and individuals if their Private Information is disclosed without authorization.

347. Progress failed to use the requisite degree of care that a reasonably prudent software company would use in designing, developing, and maintaining a secure transfer application software program.

D. Progress knew or should have known of the vulnerabilities in its software and failed to patch them.

348. SQL injection vulnerabilities, like the one exploited by Cl0p in Progress's software, are well-known vulnerabilities that Progress knew or should have known to protect against.

349. SQL injection vulnerabilities have been listed in the OWASP Top 10 vulnerabilities for many years.[338]

350. SQL injection vulnerabilities "are caused by software applications that accept data from an untrusted source (internet users), fail to properly validate and sanitize the data, and subsequently use that data to dynamically construct an SQL query to the database backing that application."[339]

351. Any data that is passed from a user to a vulnerable web application and then processed by the supporting database represents a potential attack vector for SQL injection.[340]

352. As a software development corporation, Progress was uniquely positioned to prevent SQL injection vulnerabilities.

353. Software developers like Progress are advised to employ parameterized rather than dynamic queries. Parameterized queries are simpler to write and understand and prevent the use of SQL commands inserted by an attacker.

---

[338] *See, e.g.*, OWASP Top Ten, *Top 10 Web Application Security Risks*, https://owasp.org/www-project-top-ten/ (last visited Apr. 26, 2024); *A03:2021-Injection*, OWASP Top 10: 2021, https://owasp.org/Top10/A03_2021-Injection/ (last visited Apr. 26, 2024); OWASP Top Ten, *2017 Top 10*, https://owasp.org/www-project-top-ten/2017/Top_10 (last visited Apr. 26, 2024); GitHub, https://owasp.org/www-pdf-archive/OWASP_Top_10_-_2013.pdf (last visited Apr. 26, 2024); GitHub, https://owasp.org/www-pdf-archive/OWASP_AppSec_Research_2010_OWASP_Top_10_by_Wichers.pdf (last visited Apr. 26, 2024); GitHub, https://owasp.org/www-pdf-archive/OWASP_Top_10_2007.pdf (last visited Apr. 26, 2024); OWASP Top 10, *Top 10 2004*, https://github.com/owasp-top/owasp-top-2004 (last visited Apr. 26, 2024).

[339] Chad Dougherty, *Practical Identification of SQL Injection Vulnerabilities*, US-Computer Emergency Readiness Team (2012), https://www.cisa.gov/sites/default/files/publications/Practical-SQLi-Identification.pdf.

[340] *Id.*

354. Additional standard practices to prevent SQL injection vulnerabilities include the use of stored procedures, allow-list input validation, application fuzzing, or the use of web application firewalls ("WAFs").

355. As a software developer, Progress was further in a position to mitigate the risk of SQL injection vulnerabilities by minimizing privileges assigned to each database and employing effective endpoint detection systems.

356. By failing to adhere to reasonable industry standards related to prevention of SQL injection vulnerabilities, Progress failed to use reasonable care or employ a reasonable industry standard of care for materials that it knew contained Private Information.

357. Progress's negligent acts and omissions, include, *inter alia*:

a. Negligent design of the MOVEit application;

b. Failure to utilize parameterized inquiries rather than dynamic inquiries;

c. Failure to use stored procedures;

d. Failure to utilize application fuzzing;

e. Failure to use web application firewalls;

f. Failure to conduct regular audits and penetration testing;

g. Failure to document all database accounts, stored procedures, and prepared statements along with their uses;

h. Failure to enforce best practice password and account policies;

i. Failure to use principles of least privilege;

j. Failure to ensure that error messages are generic and do not expose too much information;

k. Failure to sanitize and/or validate input;

l. Failure to deny extended URLs;

m. Failure to disable potentially harmful SQL stored procedure calls;

n. Failure to produce proactive patch production or update and patch production servers with regularity;

o. Failure to adequately secure the application and operation system;

p. Failure to deny unnecessary internet access;

q. Failure to block or restrict internet or intranet access for database systems;

r. Failure to implement firewall rules to block or restrict internet and intranet access or implement firewall rules to block known malicious IP addresses; and

s. Failure to harden internal systems against the potential threat posed by a compromised system against the potential threats poses by a compromised system on their local network.

358. Progress should have known about the vulnerabilities in the MOVEit software and was negligent in developing, maintaining, and updating the software, because:

a. Progress failed to adhere to basic, well-known industry standards for software security;

b. Progress failed to review and maintain the MOVEit Transfer code to ensure it was secure and met industry standards;

c. Progress allowed its customers to use outdated versions of MOVEit Transfer software;

d. Progress developed and maintained MOVEit Cloud without the vulnerabilities affecting MOVEit Transfer; and

e. Progress knew or should have known the consequences of its failure to follow industry standards for secure software development and maintenance.

359. Following secure software development practices from the start of development through release and continued maintenance of the software is an industry standard and best practice because it prevents the possibility of overlooking a critical security vulnerability in outdated code.[341]

[341] MOVEit Data Breach: Summary and How to Prevent SQL Injection Attacks, *supra* note 283.

360. Instead of following secure software development practices, Progress instead attempted to maintain and patch its outdated software with critical vulnerabilities, but its maintenance and patch program was ineffective.

361. As a result of its many design failures, MOVEit was effectively a trojan horse, allowing Cl0p unfettered access to the most highly sensitive and confidential data of Progress's customers.

362. Progress was further negligent in failing to timely detect and remedy the vulnerabilities in the MOVEit Transfer software, despite the fact that the vulnerability now known as CVE-2023-34362 had existed for at least two years prior to the MOVEit Data Breach.

E. Progress's failure to act as quickly as possible led to additional losses.

363. Progress's delayed disclosure and/or notification of MOVEit's critical security vulnerabilities prevented its customers from taking prompt action, including discontinuing use of MOVEit as a "secure" file transfer application. Moreover, this conduct appears to be ongoing.

364. Importantly, CVE-2023-34362 was not the only critical vulnerability in MOVEit's code.

365. In the months following the May 31, 2023, announcement of CVE-2023-34362,[342] Progress disclosed four additional SQL injection vulnerabilities, each of which would also allow a malicious actor to access, modify, and steal data within MOVEit's database. On June 9, 2023, Progress announced SQL injection vulnerability CVE-2023-35036.[343] On June 15, 2023, Progress

[342] NIST, *Progress MOVEit Transfer SQL Injection Vulnerability (CVE-2023-34362) Detail*, Nat'l Vulnerability Database (updated Apr. 25, 2024), https://nvd.nist.gov/vuln/detail/CVE-2023-34362.

[343] NIST, *Progress MOVEit Transfer SQL Injection Vulnerability (CVE-2023-35036) Detail*, Nat'l Vulnerability Database (updated Apr. 25, 2024), https://nvd.nist.gov/vuln/detail/CVE-2023-35036.

announced yet another SQL injection vulnerability, CVE-2023-35708.[344] And on July 7, 2023, Progress released a service pack that addressed three additional vulnerabilities, including two SQL injection vulnerabilities: CVE-2023-36934[345]and CVE-2023-36932.[346] The third, CVE-2023-36933,[347] would allow an attacker to trigger the application to terminate.

366. All six of the vulnerabilities, disclosed over a period of two months between May 31, 2023, and July 7, 2023, were ranked as "high" or "critical." In all cases, the original vulnerability could be exploited to upload a web shell onto the MOVEit Transfer server. The web shell allowed threat actors to enumerate files and folders on the MOVEit Transfer server, read configuration information, download files, and create or delete MOVEit server user accounts.[348]

367. Similarly, on September 27, 2023, cybersecurity researchers announced a maximum severity remote code execution vulnerability in Progress's WS_FTP file share platform. This vulnerability, CVE-2023-40044, a .NET deserialization vulnerability, allows threat actors to remotely execute commands on its operating with a simple HTTP request.

368. On September 30, 2023, cybersecurity company Rapid7 announced that it had observed multiple instances of threat actors exploiting CVE-2023-40044.

---

[344] NIST, *Progress MOVEit Transfer SQL Injection Vulnerability (CVE-2023-35708) Detail*, Nat'l Vulnerability Database (updated Apr. 25, 2024), https://nvd.nist.gov/vuln/detail/CVE-2023-35708.

[345] NIST, *Progress MOVEit Transfer SQL Injection Vulnerability (CVE-2023-36934) Detail*, Nat'l Vulnerability Database (updated Apr. 25, 2024), https://nvd.nist.gov/vuln/detail/CVE-2023-36934 (CVE-2023-36934 is a critical, unauthenticated SQL injection vulnerability).

[346] NIST, *Progress MOVEit Transfer SQL Injection Vulnerability (CVE-2023-36932) Detail*, Nat'l Vulnerability Database (updated Apr. 25, 2024), https://nvd.nist.gov/vuln/detail/CVE-2023-36932 (CVE-2023-36932 is a high-severity SQL injection vulnerability that could allow authenticated attackers to gain access to the MOVEit Transfer database).

[347] NIST, *Progress MOVEit Transfer Vulnerability (CVE-2023-36933) Detail*, Nat'l Vulnerability Database (updated Apr. 25, 2024), https://nvd.nist.gov/vuln/detail/CVE-2023-36933 (CVE-2023-36933 is an exception handling issue that could allow an attacker to crash the application).

[348] *Threat Brief – MOVEit Transfer SQL Injection Vulnerabilities: CVE-2023-34362, CVE-2023-35036 and CVE-2023-34362, CVE-2023-35036 and CVE-2023-35708*, Unit 42 (updated Oct. 4, 2023), https://unit42.paloaltonetworks.com/threat-brief-moveit-cve-2023-34362/.

369. On October 2, 2023—days after the CVE-2023-40044 vulnerability was disclosed by a third party, Progress responded by blaming security researchers for the failures of its code, announcing that it was "disappointed" that security researchers had "provided threat actors a roadmap on how to exploit the vulnerabilities" that Progress itself had created and failed to remedy.[349]

370. Rather than take responsibility for the vulnerability and their lack of disclosure, Progress blamed those who sought to inform Progress's customers. This is particularly concerning given that the MOVEit SQL injection vulnerability CVE-2023-34362 had existed for two years prior to MOVEit Data Breach.

371. According to Kroll, a "forensic review [] also identified activity indicating that the Cl0p threat actors were likely experimenting with ways to exploit this particular vulnerability as far back as 2021."[350] Other reliable cybersecurity firms have also concluded that this vulnerability was present at least as early as 2021.[351]

372. Once the first vulnerability was discovered by Progress in May of 2023, Progress should have initiated an evaluation of all its software for vulnerabilities. Likewise, Progress's announcement of the first vulnerability on May 31, 2023, should have triggered Defendants to begin taking security measures.

373. As a direct and proximate consequence of Progress's misconduct, acts, and omissions, Progress's customers have experienced direct monetary damages, including but not

[349] Sergiu Gatlan, *Exploit available for critical WS_FTP bug exploited in attacks*, BleepingComputer (Oct. 2, 2023), https://www.bleepingcomputer.com/news/security/exploit-available-for-critical-ws-ftp-bug-exploited-in-attacks/.

[350] Scott Downie, et al., *Cl0p Ransomware Likely Sitting on MOVEit Transfer Vulnerability (CVE-2023-34362) Since 2021*, Kroll (June 8, 2023), https://www.kroll.com/en/insights/publications/cyber/clop-ransomware-moveit-transfer-vulnerability-cve-2023-34362.

[351] *See* Chris Swagler, *MOVEit Data Breach: Lessons in Application Security for Modern Businesses*, Speartip (Sept. 27, 2023), https://www.speartip.com/moveit-data-breach-application-security/.

limited to: costs associated with ransomware payments, legal fees associated with incident response and regulatory concerns, costs associated with data breach response and forensic investigation, and costs associated with breach remediation and settlement of consumer claims.

374. As a direct and proximate consequence of Progress's misconduct, acts, and omissions, Progress's customers' users, including Plaintiffs and Class Members in these actions, have experienced direct and indirect monetary damages and other harm as described herein.

375. For the reasons set forth in detail above, Progess is directly liable to every member of every proposed class and faces substantial exposure – both individually and via joint and several liability – as a primary defendant in the claims stemming from the MOVEit vulnerability. Upon information and belief, Progress is able to satisfy actual or potential judgments on behalf of the proposed classes. Progress further faces actual and potential indemnification/contribution claims from its co-defendants and customers.

V. Additional Defendants are equally culpable for Plaintiffs' and Class Members' losses.

A. Defendants knew they needed to protect Plaintiffs' and Class Members' highly sensitive Private Information.

376. All Defendants—including Direct User[352] Defendants, Vendor[353] Defendants, VCE[354] Defendants, and VCE Customer Defendants[355]—knew they needed to protect Plaintiffs' and Class Members' Private Information.

[352] *See* Appendix A – Defendants' Proposed Complaint "Tracks" at 4-5 (listing "Direct User Defendants").

[353] *See id.* at 6 (listing "Vendor Defendants and associated Vendor Contracting Entities and/or Vendor Contracting Entity Customers").

[354] *See id.* (listing "Vendor Defendants and associated Vendor Contracting Entities and/or Vendor Contracting Entity Customers").

[355] *See id.* (listing "Vendor Defendants and associated Vendor Contracting Entities and/or Vendor Contracting Entity Customers").

377. Defendants were at all times fully aware of their obligations to protect the Private Information of customers and patients. Defendants were also aware of the significant repercussions that would result from their failure to do so.

378. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known they were responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized access and disclosure.

379. As a regular and necessary part of their businesses, Defendants solicit and collect the highly sensitive Private Information of patients, customers, and/or users.

380. Due to the nature of Defendants' businesses, Defendants would be unable to engage in their regular business activities without collecting and aggregating Private Information they know and understand to be sensitive and confidential.

381. Plaintiffs and Class Members relied on Defendants to implement and maintain adequate data security policies and protocols (including vetting, auditing, and monitoring vendors and software companies on which they relied) to keep their Private Information confidential and securely maintained, to use such Private Information (if at all) solely for business and healthcare purposes, and to prevent unauthorized access and disclosure of Private Information to unauthorized persons. Plaintiffs and Class Members reasonably expected Defendants would safeguard their highly sensitive information and keep that Private Information confidential.

B. Defendants knew the risks of transferring sensitive information, including the risk of data breaches.

382. Because of the highly sensitive and personal nature of the information Defendants solicit, acquire, store, and maintain with respect to patients, customers, and/or users (referred to collectively herein as "consumers") and other individuals, Defendants, upon information and

belief, promise to, among other things: keep Private Information private; comply with industry standards related to data security and Private Information, including FTC guidelines; inform consumers of their legal duties and comply with all federal and state laws protecting consumer Private Information; only use and release Private Information for reasons that relate to the products and services Plaintiffs and Class Members obtain from Defendants; and provide adequate notice to individuals if their Private Information is disclosed without authorization.

383. As sophisticated business entities handling highly sensitive and confidential consumer data, Defendants' data security obligations were particularly important, especially in light of the substantial increase in cyberattacks and data breaches in industries handling significant amounts of Private Information preceding the date of the MOVEit Data Breach.

384. At all relevant times, Defendants knew, or should have known, that Plaintiffs' and Class Members' Private Information was a target for malicious actors.

385. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class Members' Private Information from cyberattacks, including, but not limited to, adequately vetting, auditing, monitoring, testing, and patching the software applications they used to store and transfer such data.

386. In light of recent high profile data breaches—including breaches arising from previously exploited vulnerabilities in other file transfer applications (*e.g.*, Accellion FTA, Fortra GoAnywhere MFT)—Defendants knew or should have known that their electronic records and consumers' Private Information would be targeted by cybercriminals and ransomware attack groups.

387. "Third-party software security risks are on the rise, and so are the significant cyber attacks they facilitate. According to a CrowdStrike report, 45% of surveyed organizations said they experienced at least on software supply chain attack in 2021."[356]

388. Recent high profile cybersecurity incidents at healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), put Healthcare Defendants on notice that their electronic records would be targeted by cybercriminals.

389. According to the HIPAA Journal's 2023 Healthcare Data Breach Report, "[a]n unwanted record was set in 2023 with 725 large security breaches in healthcare reported to the Department of Health and Human Services Office for Civil Rights, beating the record of 720 healthcare security breaches set the previous year."[357]

390. Cyberattacks and data breaches of financial services companies or companies storing financial data are also especially problematic because of the potentially permanent disruption they cause to the daily lives of their customers. Stories of identity theft and fraud

[356] Edward Kost, *Third-Party Risk Management: How to Identify Vulnerabile Third-Party Software (Quickly)*, UpGuard (last updated Sept. 4, 2023), https://www.upguard.com/blog/how-to-identify-vulnerable-third-party-software.

[357] Steve Adler, *Security Breaches in Healthcare in 2023*, The HIPAA Journal (January 31, 2024), https://www.hipaajournal.com/wp-content/uploads/2024/01/Security_Breaches_In_Healthcare_in_2023_by_The_HIPAA_Journal.pdf.

abound, with hundreds of millions of dollars lost by everyday consumers every year as a result of internet-based identity theft attacks.[358]

391. The GAO found that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[359]

392. As highly sophisticated parties that handle sensitive Private Information, Defendants failed to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' Private Information.

393. The ramifications of Defendants' failures to keep Plaintiffs' and Class Members' Private Information secure are severe and long-lasting. To avoid detection, identity thieves often hold stolen data for months or years before using it. Also, the sale of stolen information on the "dark web" may take months or more to reach end-users, in part because the data can be sold in small batches to multiple buyers as opposed to in bulk to a single buyer. Thus, Plaintiffs and Class Members must vigilantly monitor their financial accounts, and Plaintiffs and Class Members are at an increased risk of fraud and identity theft, for many years into the future.

394. Thus, Defendants knew, or should have known, the importance of safeguarding the Private Information entrusted to them and of the foreseeable consequences if their systems were breached. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring or from mitigating the consequences of the Data Breach.

---

[358] Albert Khoury, *Scam alert: 5 most costly data breaches (plus 5 states most targeted)* (July 27, 2022), https://www.komando.com/security-privacy/most-costly-data-breaches/847800/.

[359] *See* GAO Report at 2, *supra* note 245.

C. Defendants had an obligation to carefully vet Progress's software and audit Progress's cybersecurity practices.

395. Defendants knew, or should have known, the importance of safeguarding the Private Information entrusted to them, and of the foreseeable consequences if such data were to be disclosed. These consequences include the significant costs that would be imposed on affected individuals as a result of a data breach.

396. Each Defendant therefore owed a duty to Plaintiffs and Class Members to implement and maintain reasonable and adequate data security measures to secure, protect, and safeguard the Private Information entrusted to them by Plaintiffs and Class Members.

397. Defendants should have used their resources to implement and maintain adequate data security procedures and practices.

398. Defendants breached their duties to Plaintiffs and Class Members by, among other things, failing to employ adequate vendor screening and vetting, including of Progress and its MOVEit Transfer software.

399. Defendants knew or should have known that Progress: employed poorly-written, outdated, and insecure code in its MOVEit software; failed to update outdated code; and failed to check for known or newly discovered vulnerabilities.

400. Direct User and VCE Defendants in particular should have but did not vet Progress or its MOVEit Transfer software, and as a result, failed to prevent or detect the Data Breach.

401. Direct User and VCE Defendants failed to ensure Progress employed and maintained adequate cybersecurity measures to prevent the Data Breach from occurring.

402. Defendants also had obligations arising under the FTC Act, HIPAA, industry standards, common law, and their own promises and representations made to Plaintiffs and Class

Members to keep their Private Information confidential and protected from unauthorized access and disclosure.

1. Defendants fail to comply with FTC guidelines.

403. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should factor into all business decision-making.

404. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal consumer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[360]

405. The FTC guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and, have a response plan ready in the event of a breach.[361]

406. The FTC further recommends that companies not maintain PII longer than necessary for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

---

[360] *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[361] *Id.*

407. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

408. Defendants failed to properly implement the foregoing recommended data security practices.

409. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to the Private Information in their care constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

410. Defendants were at all times fully aware of their obligations to protect the Private Information entrusted to them. Defendants were also aware of the significant repercussions that would result from their failure to do so.

2. Healthcare Defendants violated their HIPAA obligations.

411. Those Defendants who are healthcare service providers handling medical patient data and/or providing services to hospitals and healthcare organizations ("Healthcare Defendants"), are covered entities under HIPAA (45 C.F.R. § 160.103) and are required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and the HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C ("Security Standards for the Protection of Electronic Protected Health Information").

412. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

413. Healthcare Defendants are also subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. § 17921; 45 C.F.R. § 160.103.

414. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information that is kept or transferred in electronic form.

415. HIPAA covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

416. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information like the data Defendants left unguarded. The HHS subsequently promulgated multiple regulations under the authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306 (a)(1-4); 45 C.F.R. § 164.312 (a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308 (a)(1)(ii)(D); and 45 C.F.R. § 164.530(b).

417. The MOVEit Data Breach as to certain Defendants is considered a breach under the HIPAA Rules because it involved an access of PHI not permitted under the HIPAA Privacy Rule:

418. A breach under the HIPAA Rules is defined as "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40.

419. The MOVEit Data Breach resulted from a combination of insufficiencies that demonstrate Healthcare Defendants failed to comply with safeguards mandated by HIPAA regulations.

420. As HIPAA covered business entities, Healthcare Defendants are required to implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Private Information, including incidents that constitute breaches of unsecured PHI, as in the case of the MOVEit Data Breach.

421. As HIPAA-covered entities handling medical patient data, Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and data breaches in the healthcare industry and other industries holding significant amounts of PII and PHI preceding the date of the Data Breach.

3. Defendants failed to comply with industry standards.

422. Several best practices have been identified that at a minimum should be implemented by entities, like Defendants, that handle highly sensitive and confidential Private Information.

423. These best practices include, but are not limited to: educating all employees about data security practices and procedures; requiring strong passwords; implementing multi-layer security—including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

424. Other standard cybersecurity practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers;

monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

425. On information and belief, Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

426. These foregoing frameworks are existing and applicable industry standards, and Defendants failed to comply with these accepted standards, thereby opening the door to Cl0p and causing the Data Breach.

D. Had Defendants taken their obligations seriously, they would have determined that the MOVEit software was not safe to use.

427. Defendants are responsible for protecting the Private Information they solicit and collect from attacks and breaches that result from weaknesses in third-party systems and software.

428. Defendants failed to safeguard Plaintiffs' and Class Members' Private Information when they failed to adopt and enforce reasonable and available data security practices and procedures to prevent and/or mitigate the known risk of a cyberattack.

429. Prior to the Data Breach, Defendants should have, but did not, implement and maintain reasonable and necessary data security policies and procedures, which would have mitigated or avoided the Data Breach.

430. There are numerous known and available steps that Defendants could have taken to mitigate or even prevent the Data Breach.

431. Data security practices that could and should have been implemented by Defendants to prevent the MOVEit Data Breach include:

a. Auditing of third-party software, including the MOVEit Transfer software;

b. Vetting and periodic auditing of third-party vendors, including Progress;

c. Restricting MOVEit transfers to pre-approved IP addresses ("whitelisting");

d. Limiting the specific types of files that can be uploaded;

e. Conducting basic monitoring of web servers;

f. Using web application firewalls ("WAFs"); and

g. Employing supply chain security.

1. Auditing Third-Party Software.

432. Security audits of third-party software enable companies to identify vulnerabilities, monitor access to sensitive data, and discover and remediate any unauthorized data access.[362] Here, security auditing of the MOVEit Transfer software could have prevented the Data Breach. The methods for conducting security audits of third-party software are well-known and widely available.[363] Defendants therefore could and should have employed companies that conduct security audits of third-party software.[364]

2. Vetting Vendors.

433. In addition to auditing third-party software, proper vetting and routine audits of vendors' data security practices, including vetting of Progress's cybersecurity practices, could

[362] *6 Security Tips for Third Party* Software, Cybersecurity Insiders, https://www.cybersecurity-insiders.com/6-security-tips-for-third-party-software/ (last visited May 20, 2024).

[363] Edward Kost, *Third-Party Risk Management: How to Identify Vulnerable Third-Party Software (Quickly)*, UpGuard (updated Sept. 4, 2023), https://www.upguard.com/blog/how-to-identify-vulnerable-third-party-software.

[364] Davit Asatryan, *Third-Party Applications Audit: Complete Guide*, Spin.ai (Nov. 4, 2021, updated Apr. 19, 2024), https://spinbackup.com/blog/third-party-applications-audit/.

have prevented the Data Breach. Vendor risk assessments or security questionnaires are "one of the best methods for extracting deep cybersecurity insights about any aspects of a vendor's attack surface."[365] Industry-standard risk assessments and security questionnaires designed to help companies discover vulnerabilities in third-party web applications and software are widely available,[366] and can be used to assess the security of third-party software against common attack vectors, including SQL injection susceptibility.[367]

3. Whitelisting.

434. Restricting MOVEit transfers to pre-approved IP addresses—a cybersecurity practice referred to as "whitelisting"—could also have prevented the Data Breach. A whitelist is an administrator-defined register of entities pre-approved for authorized access or to perform specific actions. Whitelisting enhances the security of a system or network by ensuring that only pre-approved users or devices have access to sensitive data or systems. Whitelisting thus denies access by default, providing authorization only to a vetted, pre-approved list of IP addresses, applications, email addresses, and/or users. Blacklisting, in contrast, requires that known threats be specifically identified and blocked, while everything else is permitted. By definition, a blacklist cannot protect against an exploitation of a Zero-Day vulnerability, like the one Cl0p exploited in the MOVEit Data Breach. NIST Special Publication 800-167: *Guide to Application Whitelisting* provides specific guidance to companies on how to implement whitelisting.[368]

---

[365] Edward Kost, *Third-Party Risk Management: How to Identify Vulnerable Third-Party Software (Quickly)*, UpGuard (updated Sept. 4, 2023), https://www.upguard.com/blog/how-to-identify-vulnerable-third-party-software ("Risk assessments can either be framework-based to identify security control deficiencies against popular security standards or custom-designed for focused investigations about specific third-party risks.").

[366] *Id.*

[367] *Id.*

[368] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf.

4. Limiting Specific File Types.

435. Limiting the specific types of files that can be uploaded via FTP could also have prevented the Data Breach. After exploiting the MOVEit vulnerability via SQL injection, Cl0p uploaded the LEMURLOOT web shell, which masqueraded as a legitimate file[369] and allowed the threat actor to execute commands, download files, extract system settings, and create/insert/delete users.[370]

436. Proper data security dictates that only those files that are needed and expected to be uploaded should be allowed. This typically includes document file types such as .doc, .docx, .pdf, etc. Only web site administrators with whitelisted IP addresses should have been allowed to upload web page files, such as .aspx.

5. Adequate Logging, Monitoring, and Auditing.

437. "Logging, monitoring, and auditing procedures help an organization prevent incidents and provide an effective response when they occur."[371] These tools can detect SQL injection attempts and mitigate or even prevent breaches like the MOVEit Data Breach.

438. Forensic examinations of the MOVEit Data Breach have confirmed that indicators of compromise were found in the logs of targeted organizations,[372] verifying that effective log monitoring would have mitigated or even prevented the Data Breach. Accordingly, Defendants

[369] https://blog.qualys.com/vulnerabilities-threat-research/2023/06/07/progress-moveit-transfer-vulnerability-being-actively-exploited; *see also* https://securityintelligence.com/news/the-moveit-breach-impact-and-fallout-how-can-you-respond/.

[370] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

[371] Mike Chapple, et al., (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide (9th ed. 2021).

[372] Scott Downie, et al., *Transfer Vulnerability (CVE-2023-34362) Since* 2021, Kroll (June 8, 2023), https://www.kroll.com/en/insights/publications/cyber/clop-ransomware-moveit-transfer-vulnerability-cve-2023-34362.

could and should have utilized commonly available tools that monitor logs automatically and provide alerts of unusual activity to administrators.

439. "Several different logs record details of activity on systems and networks. For example, firewall logs record details of all traffic that the firewall blocked. By monitoring these logs, it's possible to detect incidents. Some automated methods of log monitoring automatically detect potential incidents and report them right after they've occurred."[373]

440. Here, adequate logging and log monitoring could have prevented the MOVEit Data Breach because logs would have shown clear indicators of compromise and/or malicious activity. SQL injection attempts, successful or not, will appear in such logs. But even extensive logging is insufficient without adequate monitoring of said logs.

441. The U.S. National Institute of Standards and Technology (NIST) publishes a Cybersecurity Framework that emphasizes continuous monitoring of systems.[374] The NIST SP 800-92 Guide to Computer Security Log Management further defines how to manage logs,[375] and there are a number of widely available tools that can monitor logs automatically and provide alerts to administrators when there is unusual activity.

442. Monitoring web server logs for new files, as recommended in NIST SP 800-12,[376] is a widely accepted cybersecurity practice[377] that would have promptly detected the new files

[373] Darril Gibson, CompTIA Security+ Get Certified Get Ahead: SY0-501 Study Guide at p. 73 (2017).

[374] NIST, *The NIST Cybersecurity Framework (CSF) 2*.0, Nat'l Inst. of Standards and Tech. (Feb. 26, 2024), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

[375] NIST, *Guide to Computer Security Log Management*, Nat'l Inst. of Standards and Tech. (Sept. 2006), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf.

[376] NIST, *An Introduction to Information Security*, NIST Special Publication 800-12, Rev. 1 (June 2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf.

[377] *Monitor web server directories for changed / new files*, https://serverfault.com/questions/1145284/monitor-web-server-directories-for-changed-new-files (last visited May 20, 2024); *Gateway Script to monitor directory for new files*, Ignition https://forum.inductiveautomation.com/t/gateway-script-to-monitor-directory-for-new-files/16124/5 (last visited May 20, 2024).

introduced in the MOVEit Data Breach. Web server monitoring would have specifically allowed Defendants to detect the new files introduced to the web server root (human.aspx and human2.aspx) that enabled Cl0p to perpetrate the MOVEit Data Breach. Even basic monitoring of Defendants' web servers could therefore have prevented the Data Breach because it would have revealed the backdoor Cl0p introduced to the web server.[378]

443. In addition to file system monitoring to identify new files, the InfoSec institute recommends: (a) network monitoring to identify rogue IP addresses which may be performing malicious activities such as brute-force or fuzzing; (b) authentication monitoring to identify unusual logins or login attempts; (c) file change monitoring to identify changes to sensitive files within the file system; and (d) process monitoring to identify rogue processes that might be malicious.[379]

444. Beyond monitoring activity, the actual data transferred via MOVEit could and should have been monitored by Defendants. Most legitimate interactions utilizing MOVEit only upload or download relatively small amounts of data at a given time, but Cl0p was able to exfiltrate large amounts of consumer data in the Data Breach. Had Defendants been adequately monitoring data transfers, any attempt to exfiltrate large amounts of data (significantly varying from normal usage) would have triggered an alert.

[378] Tyler Lioi, *MOVEit Transfer Investigations*, CrowdStrike Blog (June 5, 2023), https://www.crowdstrike.com/blog/identifying-data-exfiltration-in-moveit-transfer-investigations/.

[379] Lester Obbayi, *Web server protection: Web server security monitoring*, InfoSec (May 4, 2020), https://www.infosecinstitute.com/resources/network-security-101/web-server-protection-web-server-security-monitoring/.

6. WAFs

445. Properly configured web application firewalls ("WAFs") could also have prevented or mitigated the effects of the MOVEit Data Breach.[380]

7. Supply Chain Security

446. Supply chain security is another common method of ensuring that all items in the supply chain, including third-party software like MOVEit, is secure.[381]

447. The National Institute of Standards and Technology explicitly discusses vulnerabilities in third party software[382] and provides three supply chain security principles[383] that, if applied, would have mitigated or prevented the MOVEit breaches:

Figure 13

Cyber Supply Chain Security Principles:

1. **Develop your defenses based on the principle that your systems will be breached**. When one starts from the premise that a breach is inevitable, it changes the decision matrix on next steps. The question becomes not just how to prevent a breach, but how to mitigate an attacker's ability to exploit the information they have accessed and how to recover from the breach.
2. **Cybersecurity is never just a technology problem, it's a people, processes and knowledge problem**. Breaches tend to be less about a technology failure and more about human error. IT security systems won't secure critical information and intellectual property unless employees throughout the supply chain use secure cybersecurity practices.
3. **Security is Security.** There should be no gap between physical and cybersecurity. Sometimes the bad guys exploit lapses in physical security in order to launch a cyber attack. By the same token, an attacker looking for ways into a physical location might exploit cyber vulnerabilities to get access.

[380] *See, e.g.*, *Web Application Firewall*, Imperva, https://www.imperva.com/products/web-application-firewall-waf/ (last visited Apr. 26, 2024); Huawei Cloud, *How Does WAF Detect SQL Injection, XSS, and PHP Injection Attacks?* (Sept. 6, 2023), https://support.huaweicloud.com/intl/en-us/waf_faq/waf_01_0457.html.

[381] NIST, *Best Practices in Cyber Supply Chain Risk Management*, https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf (last visited Apr. 26, 2024).

[382] NIST, *Best Practices in Cyber Supply Chain Risk Management – Conference Materials*, https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf (last visited May 20, 2024).

[383] *Id.*

8. Windows Security Feature

448. Defendants utilizing Windows have an additional protection modality. The Windows security system has ransomware protection, which allows the user to designate any folder as protected. Any attempt to add new files or change existing files in that folder would then have to be approved. Because LEMURLOOT masqueraded as a legitimate file that was then used as a backdoor, having the folder \inetpub\wwwroot\ protected from alterations would have prevented these files from being uploaded.

449. In addition to the foregoing data security practices, which, if adopted by Defendants, could have prevented the Data Breach, there are a number of common security techniques and mechanisms that should be a part of any standard data security policy and could have limited the scope of damage from a data breach. These security techniques and practices include:

a. Limiting access by employing a "least privileges" policy;

b. Implementing "zero-trust" security frameworks;

c. Encrypting data at rest; Immediately applying patches once they were made available.

450. A "least privileges" policy can limit an attacker who exploits a vulnerability from accessing large volumes of data. Limiting access via policies such as least privileges means that, even if a threat actor is able to exploit a vulnerability or even use a legitimate login to access the system, access to sensitive data will be limited. The large volume of records accessed and exfiltrated in the Data Breach indicates that this was not done, because it is highly unlikely that any login would have legitimate access to that amount of sensitive data.

451. "Zero Trust" is a security model and set of system design principles that emphasize security verification in network environments. The core principle of Zero Trust is "never trust,

always verify." Thus, unlike traditional security models that assume everything inside a network is safe, Zero Trust assumes threats can exist both inside and outside the network.

452. Zero Trust security frameworks require all users, whether inside or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted access to applications and data.[384] Numerous standards provide guidelines to organizations implementing "zero-trust" security frameworks, including NIST SP 800-207,[385] NIST SP 800-205,[386] and the CISA zero trust maturity model.[387]

453. Two aspects of Zero Trust are particularly applicable to the MOVEit Data Breach. The first is the network is segmented into smaller, secure zones to maintain separate access for different parts of the network. This reduces the lateral movement of attackers within the network. The second is continuously monitoring the security posture of all hardware and software on the network. This helps to detect and respond to threats in real time.

454. Encrypting data at rest is a common data security practice[388] specifically recommended to mitigate SQL injection attacks.[389] Encrypting files and databases at rest prevents threat actors who gain access to a system from accessing sensitive data on the system without a

---

[384] *See, e.g.*, *Zero Trust, A revolutionary approach to Cyber or just another buzz word?*, Deloitte (2021), https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/deloitte-cyber-zero-trust.pdf; *see also* Venu Shastri, *Zero Trust Architecture*, CrowdStrike (June 28, 2023), https://www.oracle.com/security/what-is-zero-trust; https://www.crowdstrike.com/cybersecurity-101/zero-trust-security.

[385] NIST, *NIST SP 800-207 – Zero Trust Architecture*, CSRC (Aug. 2020), https://csrc.nist.gov/pubs/sp/800/207/final.

[386] NIST, *NIST SP 800-205 – Attribute Considerations for Access Control Systems*, CSRC (June 2019), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-205.pdf.

[387] *Zero Trust Maturity Model*, CISA (Apr. 2023), https://www.cisa.gov/sites/default/files/2023-04/CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf.

[388] *See, e.g.*, Scott Myers, *Securing Data at Rest with Encryption*, Ingalls (Apr. 20, 2022), https://blog.iinfosec.com/securing-data-at-rest-with-encryption; *SQL Injection Attacks (SQLi)*, Rapid 7, https://www.rapid7.com/fundamentals/sql-injection-attacks/ (last visited May 20, 2024); https://www.ijert.org/research/prevention-of-sql-injection-attacks-using-rc4-and-blowfish-encryption-techniques-IJERTV5IS060092.pdf.

[389] Sonakshi, et al., *Prevention of SQL Injection Attacks using RC4 and Blowfish Encryption Techniques*, 5 Int'l J. of Engineering Research & Tech. 6 (June 2016), https://repository.stcloudstate.edu/cgi/viewcontent.cgi?article=1105&context=msia_etds.

cryptographic key and is required or recommended by numerous standards, including PCI-Data Security Standards,[390] SOC 2,[391] and NIST SP 800-53.[392] The standard NIST SP 800-53 explicitly recommends encrypting data at rest in section SC-28.[393]

455. PCI-DSS specifically recommends encryption of data and data masking. Protection methods such as encryption, truncation, masking, and hashing are critical components of account data protection. If an intruder circumvents other security controls and gains access to encrypted account data, the data is unreadable without the proper cryptographic keys and is unusable to that intruder.

456. The United States Cybersecurity & Infrastructure Security Agency published recommendations for mitigating the MOVEit vulnerability by "[g]rant[ing] admin privileges and access only when necessary, establishing a software allow list that only executes legitimate applications."[394]

457. Finally, following Progress's announcement of the first MOVEit vulnerability on May 31, 2023,[395] Direct User Defendants should have, but did not, immediately begin taking security measures. Defendants' failure to adequately safeguard Plaintiffs' and Class Members' Private Information resulted in that information being accessed or obtained by third-party cybercriminals.

---

[390] PCI, Document Library, https://east.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss (last visited May 20, 2024).

[391] *SOC2 Compliance – The Definitive Guide*, A-LIGN, https://www.a-lign.com/resources/soc-2-the-definitive-guide (last visited May 20, 2024).

[392] NIST, *NIST SP 800-53 – Security and Privacy Controls for Information Systems and Organizations*, U.S. Dep't of Commerce (Sept. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[393] *Id.*

[394] *#StopRansomware: Cl0p Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability*, CISA (June 7, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

[395] *MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362)*, *supra* note 126.

E. Defendants failed to follow Progress's recommendations regarding secure configuration of the MOVEit software.

458. The MOVEit software offers secure configurations that any customer could implement to make the system more secure and to mitigate that impact of this breach.

459. Progress made several additional recommendations to users of the MOVEit software, including:

a. Using consistency check and tamper check utilities to validate consistently and the audit log.

b. Review audit logs for any anomalous behavior. Such anomalous behavior includes:

i. Sign-ons from specific IP addresses

ii. APIs used

iii. Modification of settings

c. Limiting administrative privileges.[396]

d. IP and user lockout policies.[397]

e. Whitelisting so only specific IP addresses and users could login remotely.[398]

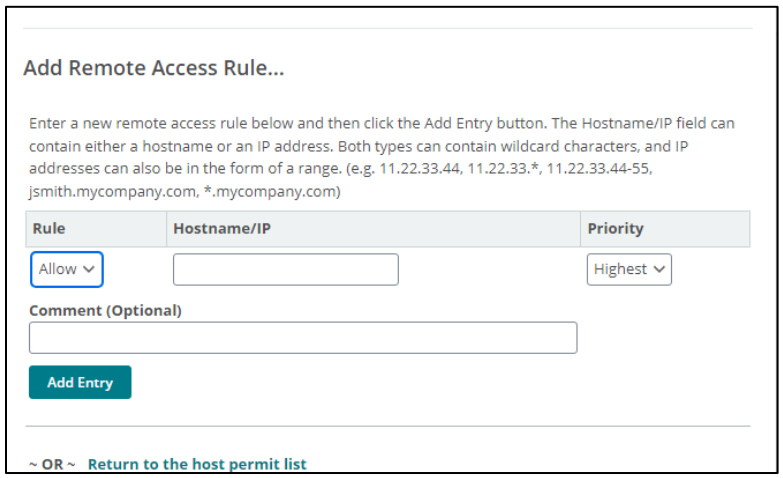
460. Defendants could and should have turned on whitelisting:

[396] *Progress Documentation: MOVEit Transfer 2022 Administrator Guide*, Progress (updated Apr. 6, 2022), https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2022/page/Permissions_3.html.

[397] *Progress Documentation: MOVEit Automation Web Admin Help – IP/User Lockout Policy*, Progress (updated Feb. 21, 2022), https://docs.progress.com/bundle/moveit-automation-web-admin-help-2022/page/IPUser-Lockout-Policy.html.

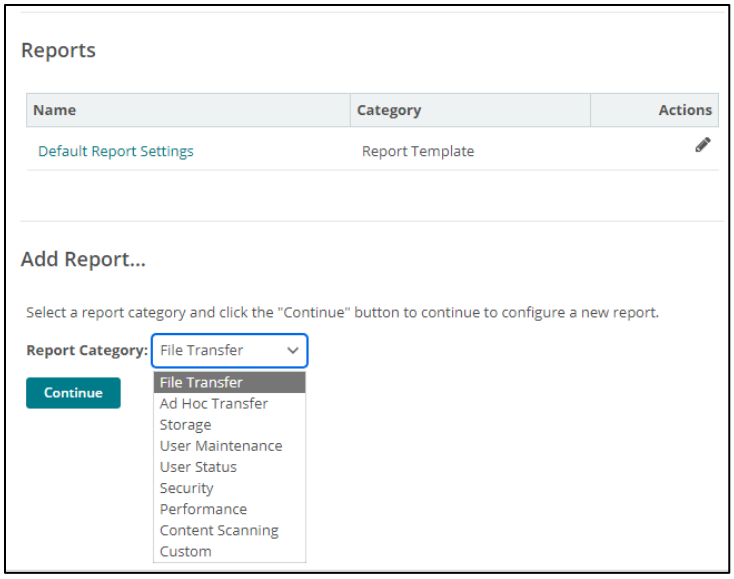
[398] *MOVEit Transfer – Whitelist IP for Specific Users Accounts*, Progress: Community (Oct. 14, 2020), https://community.progress.com/s/article/moveit-transfer-whitelist-ip-for-specific-users-accounts.

Figure 14



461. Generating reports in MOVEit is also a simple process:

Figure 15



462. There are a number of security reports built into the MOVEit software:

Figure 16

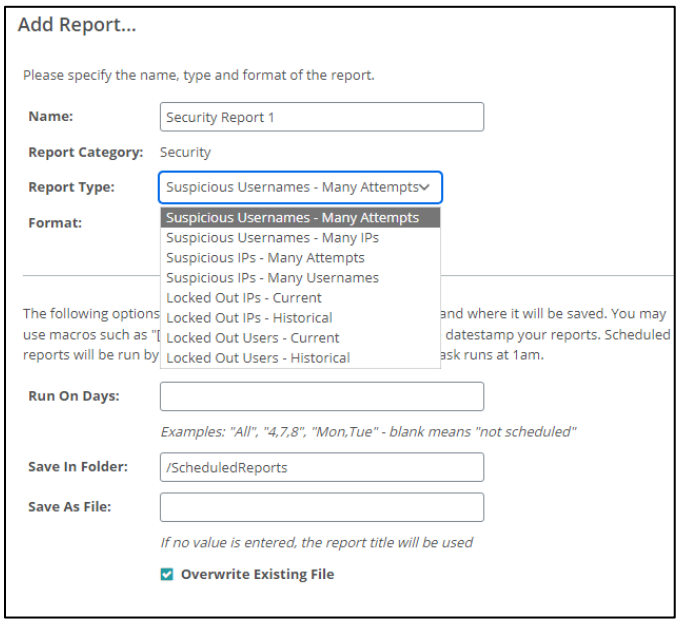
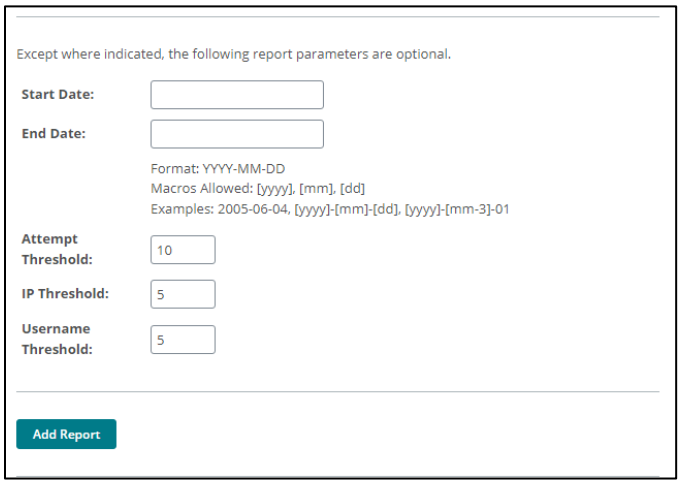
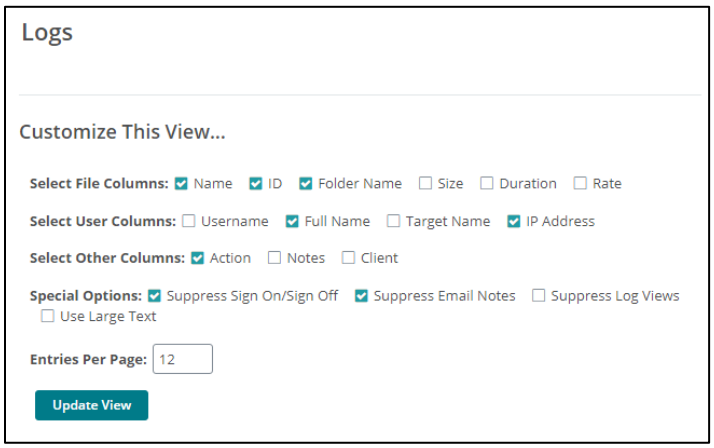


Figure 17



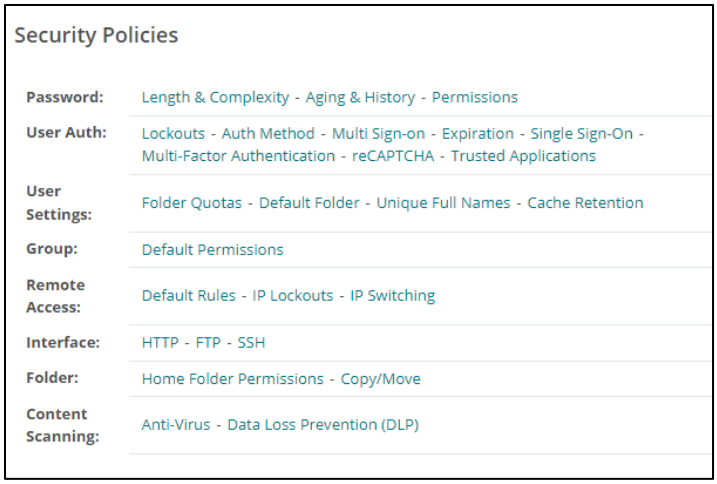
463. MOVEit users can also customize the view of logs:

Figure 18



464. A number of additional security policies can be set with a simple point and click:

Figure 19



465. Data loss prevention rules could and should have been enabled to prevent exfiltration of data:

Figure 20

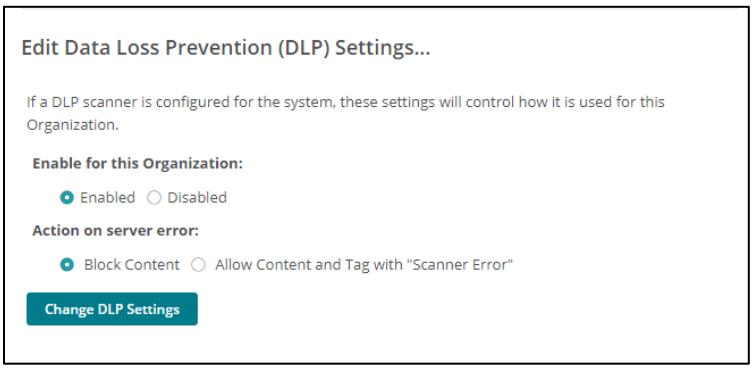


Figure 21

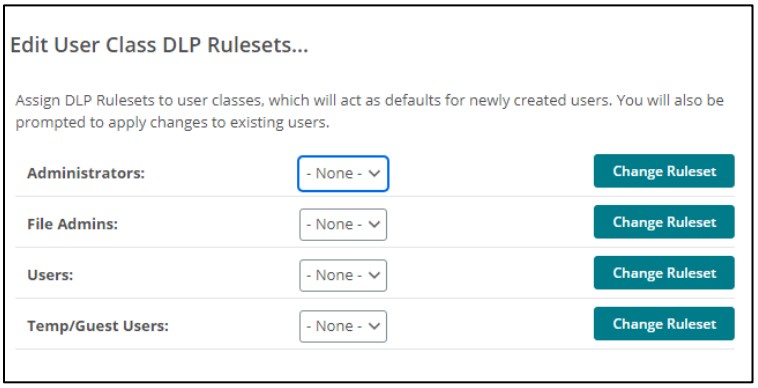
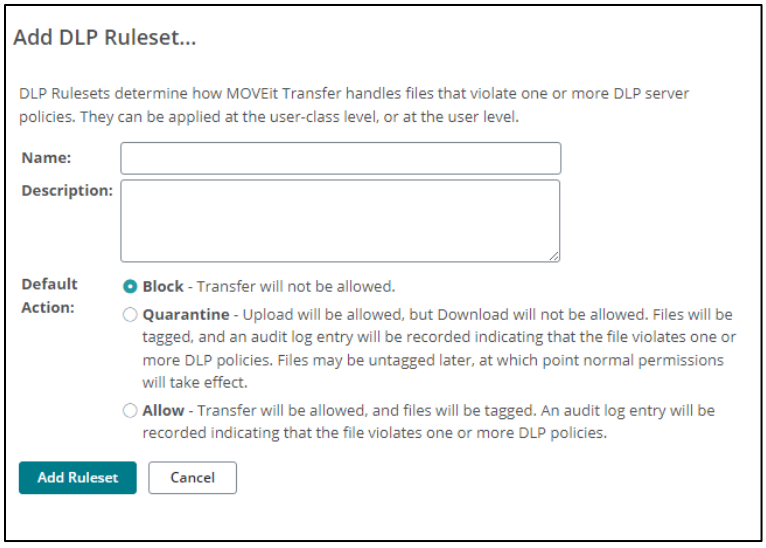


Figure 22



466. It is unclear which, if any, of these security measures were implemented by Defendants.

F. Defendants chose to use the MOVEit software to transfer sensitive information despite its security flaws.

467. Defendants enriched themselves by saving the costs they reasonably should have expended on adequate data security measures to secure Plaintiffs' and Class Members' Private Information.

468. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to avoid their data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' failures to provide the requisite security.

Dated: May 24, 2024

Respectfully submitted,

By: /s/ *Kristen A. Johnson*
Kristen A. Johnson (BBO# 667261)
HAGENS BERMAN SOBOL SHAPIRO LLP
1 Faneuil Hall Square, 5th Fl.
Boston, MA 02109
Tel: (617) 482-3700
Fax: (617) 482-3003
kristenj@hbsslaw.com

Liaison & Coordinating Counsel

By: /s/ *E. Michelle Drake*
E. Michelle Drake
BERGER MONTAGUE, PC
1229 Tyler St., NE, Ste. 205
Minneapolis, MN 55413
Tel: (612) 594-5933
Fax: (612) 584-4470
emdrake@bm.net

By: /s/ *Gary F. Lynch*
Gary F. Lynch
LYNCH CARPENTER, LLP
1133 Penn Ave., 5th Fl.
Pittsburgh, PA 15222
Tel: (412) 322-9243
Fax: (412) 231-0246
Gary@lcllp.com

By: /s/ *Douglas J. McNamara*
Douglas J. McNamara
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Ave. NW, 5th Fl.
Washington, DC 20005
Tel: (202) 408-4600
dmcnamara@cohenmilstein.com

By: /s/ *Karen H. Riebel*
Karen H. Riebel
LOCKRIDGE GRINDAL NAUEN PLLP
100 Washington Ave. S., Ste. 2200
Minneapolis, MN 55401
Tel: (612) 339-6900
Fax: (612) 612-339-0981
khriebel@locklaw.com

By: /s/ *Charles E. Schaffer*
Charles E. Schaffer
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Ste. 500
Philadelphia, PA 19106
Tel: (215) 592-1500
Fax: (215) 592-4663
cshaffer@lfsblaw.com

Lead Counsel

CERTIFICATE OF SERVICE

I hereby certify that, on this date, the foregoing document was filed electronically via the Court's CM/ECF system, which will send notice of the filing to all counsel of record.

Dated: May 24, 2024

/s/ Kristen A. Johnson
Kristen A. Johnson (BBO# 667261)