Court File No. CV-24-00000869-0000

ONTARIO
SUPERIOR COURT OF JUSTICE

B E T W E E N:

GULED WARSAME and SHELLI SAREEN on their own behalf and on behalf of all members of UNITE HERE Local 75

Plaintiffs

and

DAVID SANDERS, ASHLEY HAYES, RAFUNZEL KORNGUT AND ALLAN PACE on his own behalf and on behalf of all members of THE TORONTO HOSPITALITY EMPLOYEES UNION – CSN (THEU-CSN)

Defendants

INDEX

Court File No. CV-24-00000869-0000

ONTARIO
SUPERIOR COURT OF JUSTICE

B E T W E E N:

GULED WARSAME and SHELLI SAREEN on their own behalf and on behalf of all members of UNITE HERE Local 75

Plaintiffs

and

DAVID SANDERS, ASHLEY HAYES, RAFUNZEL KORNGUT AND ALLAN PACE on his own behalf and on behalf of all members of THE TORONTO HOSPITALITY EMPLOYEES UNION – CSN (THEU-CSN)

Defendants

AFFIDAVIT OF LINDSAY HEIDKER
(SWORN JUNE 5, 2024)

I, Lindsay Heidker, of the City of Toronto, in the Province of Ontario, MAKE AN OATH AND SAY:

1. I am employed as a law clerk with the law firm of Cavalluzzo LLP, lawyers for the Plaintiffs in the Action styled above and, as such, have knowledge of the matters deposed to herein.

2. On May 31, 2024, our office retained the services of Ellwood Evidence Inc. On June 4, 2024, our office was provided with a letter from Ellwood Evidence Inc.. Attached hereto as **Exhibit "A"** is a copy of this letter.

3. I make this Affidavit *bona fide*.

SWORN BEFORE ME by video conference from the City of Toronto, in the Province of Ontario, to the City of Pickering, in the Regional Municipality of Durham, on June 5, 2024, in accordance with O. Reg. 431/20.

Commissioner for Taking Affidavits

Christina Shiwsankar
a Commissioner, etc. for the
Province of Ontario
while being a licensed Paralegal

LINDSAY HEIDKER

This is **Exhibit "A"** referred to in the Affidavit of Lindsay Heidker, sworn June 5, 2024.

Commissioner for Taking Affidavits (or as may be)

Christina Shiwsankar
a Commissioner, etc. for the
Province of Ontario
while being a licensed Paralegal

William B. Ellwood
Senior Investigator
Court Certified Digital Forensic Examiner
+1.416.410.1441
wellwood@ellwood.com

CLLP240531

June 3rd, 2024

Stephen J. Moreau
Cavalluzzo LLP
Barristers & Solictors
300 – 474 Bathurst St.
Toronto ON M5T 2S6

RE: **Information Identification, Recovery and Remediation**

Dear Stephen,

I am the senior investigator at ellwood Evidence Inc. I have personally engaged in many of projects involving data exfiltration as an expert over the past 12 years. I have provided my resume as appendix "A".

ellwood Evidence works as a team on its assignments. I provide the following web link to the resumes of our team here, Team — ellwood Evidence Inc, https://www.ellwoodevidence.com/team.

Definitions

The **Breach Data** – There is data said to be the property of Guled Warsame and Shelli Sareen on their own behalf and on behalf of all members of Unite Here Local 75 (the **Plaintiffs**). It is claimed that this data was exfiltrated from the care and control of Plaintiffs.

Local 75 – Local 75 refers to the Unite Here union, chapter known as Local 75.

The **Parties Holding the Breach Data** - This term will refer to the Defendants who are, David Sanders, Ashley Hayes, Rafunzel Korngut and - Allan Pace on his own behalf and on behalf of all members of The Toronto Hospitality Employee Union – CSN. It will also include those other parties that received the Breach Data directly or indirectly as a result of the actions of Defendants. Some Parties Holding the Breach Data may not be aware that the data they hold is the property of the Local 75. The Parties Holding the Breach Data may be individuals, or they may be organizations.

Scope of Work

You have asked us to provide an outline of the actions required to identify, copy and, ultimately, remove the Breach Data that is claimed to be the property of the Plaintiffs, that is found to be or to have been in the possession or control of the Parties Holding the Breach Data.

Challenges

Data can be Easily Copied

A copy of a digital record or file is identical to the original, copying data is practically costless, and data can be copied from one device to another effortlessly at any time.

An Order may be requested that directs the defendants and those other parties that may hold or control any of the Breach Data from making copies of the Breach Data or deleting it from where they encounter it.

Short Lived Audit Logs

This Order may also require the defendants and those other parties to preserve their system logs and audit data of computer system activity including those on personal computers, file servers, databases, and cloud-based storage systems. Audit logs will often be set to automatically delete after a specific number of days as part of the ordinary course of business. These automated deletion processes should be Ordered to be paused immediately to preserve this potential evidence.

An Order allowing a third-party access to these various logs should be made to allow the third-party to observe the activity around the Breach Data. These records will help determine what devices store the Breach Data.

Databases

Databases can be used to comingle the Breach Data with data legitimately held by the Parties Holding the Breach Data. Databases are often complex and proprietary in their structure.

An Order directing those with knowledge of the relevant databases to assist with the search process will be important to ensure these databases are properly canvased.

Personal Devices

The organization where the Breach Data may be stored may allow their employees and contractors to hold organizational data on their personal devices. If that is the case, then the Breach Data may have migrated to some of these personal devices.

Some organizations permit use of personal devices, but they require employees and contractors of acknowledge that in doing so the employee or contractor will permit search of these devices as required. In other cases, employees and contractors are given no such requirement and may decline to offer devices for search.

An Order compelling those personal devices that may hold the Breach Data would be appropriate.

Staff Turn Over

Employees and contractors with knowledge of the Breach Data may no longer be affiliated with the organization(s) that may be thought to be holding the Breach Data.

An Order requiring the cooperation of these parties may facilitate a broader understanding of how the data was acquired and how it was used, leading to where it may be stored.

Privacy Concerns and Minimize Intrusion

A search for the Breach Data will necessarily engage with storage devices and systems that contain private information that does not pertain to Local 75. It will also contain information that is part of the confidential information of the organization being searched.

The searching process must take great care to ensure that private and confidential information is not exposed in the search and collection process to the extent that can be accomplished.

Where the Breach Data is found to be comingled an external third-party review might be required to protect privacy and confidentiality.

It may be that many of the Parties Holding the Breached Data are doing so not by their own volition but instead by the circumstances of receiving data that to their knowledge was innocently obtained. The intrusion to these innocent Parties Holding the Breached Data must be minimized where possible.

Adaptability

While all parties will want an agreement setting out the exact locations to search, the custodians involved and the terms to be used at the outset, the process of identification and search as it progresses will inform subsequent steps and the scope of the identification and search work.

With so much uncertainty at the outset, direction, in the form of an agreement between the parties or an Order from the court, needs to provide for flexibility within the principles of reasonableness balanced with privacy and confidentiality concerns.

Identification

Local 75, the rightful owner of the Breach Data, does not know where the Breach Data is. Local 75 became aware of the loss of their data when some of it was used by another organization to engage with some of Local 75's membership.

What is the Character of the Data?

The first step in the process is to determine what types of data Local 75 was holding at the time of the departure of the some of the defendants.

To do this, we will interview some of the Local 75 leadership and staff to understand their data management processes, storage locations and security restrictions in place in 2017, before and at the time of the departures.

Key systems will include:

- Membership management systems,
- Contact management systems,
- Outreach and Marketing systems,
- Data file storage systems,
- Other systems that interact with member information,
- Email systems,
- Among others.

We will be asking for criteria we can use to search for the Breached Data. This criterion may include:

- Names and other personal information of the membership,
- Contract numbers, and other information that pertains to contracts,
- Other information the Local 75 team feels relevant to a search.

Where might Parties Holding the Breach Data have stored it?

There may be files, emails, information management systems and databases, hosted locally on local workstations and file servers and/or stored in internet-based locations like DropBox, Microsoft 365, Google, and other such services.

We will need to interview the Parties Holding the Breach Data and their support staff, like IT and marketing personnel, to gain an understand of what needs to be searched to learn the possible locations of the Breach Data.

Search

Locations to Search

The process of interviews described above can allow the search to be focused on specific systems and storage locations. This is the path of minimal invasiveness.

Inclusive Search Terms

With potential locations of the data, and the form in which the data might be stored having been established in the identification phase, the criteria to be used to identify potential Breach Data can be set out and agreed by the parties or order by the court.

Key terms will include the contact information of those Local 75 members that have been identified as having been contacted by other organizations where there is no explanation around how their contact information came into the hands of that organization.

It may be that the search terms will include contact information of all the membership of Local 75 along with contract details with Local 75 sites and other information Local 75 believes is relevant.

Time Range

It may be that data that meets the search criteria pre-dates the departure of the earliest defendant from Local 75. If so, this data is unlikely to be part of the Breach Data. But perhaps data was being provided earlier than their departure date. Therefore, the parties should agree on some date prior to the earliest departure that could be used in the search process to rule out certain responsive data.

Exclusion Terms

There may be no forward end date for the Time Range as the Breach Data may continue to be used actively. However, some of the inclusive search terms may hit upon data that is protected by Solicitor/Client privilege.

Terms that would trigger the implication of such privilege should be provided and agreed upon by the parties.

Search Methodology

Using the search criteria we will deploy in-place data assessment tools on end-user workstations, laptops and file shares of all kinds.

Where the data assessment tools can read database content, including email systems, these tools will be deployed against them. Where the database information is not accessible by data assessment tools, a review of these databases can be performed using database search tools with the assistance of the Parties Holding the Breach Data or their support staff.

Cloud and other Hosted data sets can be searched using various tools, either native to the hosted application or with separate tools designed for the purpose, as is appropriate. These systems might include hosted mass emailing systems like MailChimp and others along with hosted Customer Management Systems (CRMs), file storage systems, backup systems and alike.

Search generally proceeds in two stages. The first stage is the execution of the tools to create a searchable index of the content. The second stage is using the index to perform the searches according to the search criteria. While indexing does take significant time, the systems themselves remain available to their users during the indexing process with only a minor reduction in performance.

Review

Knowing what data was taken from Local 75 and how it was used will assist their counsel in evaluating the damages associated with the Breach.

Local 75 may also have Privacy Commission issues to deal with around the loss of personal information of their membership. They may have some obligations around reporting to the Privacy Commission and taking their direction around disclosure to the membership.

Part of the process will be to copy out and create a data set responsive to the Inclusive Search Terms, and Time Range, abstracting out the materials also responsive to the Exclusion Terms (**Recovered Breach Data**).

An analysis of the Recovered Breach Data will be performed to provide these insights to Local 75.

An order from the court may require or the parties may agree that an independent third-party perform a review of the Recovered Breach Data to ensure that it is appropriately designated as such.

Expungement

The Recovered Breach Data, once parties or the court agree on its corpus, can then be securely removed from the systems where it was found.

Simple secure deletion of files can take place. Email systems, databases, backup systems, and cloud-based information systems will have to be considered to achieve effective expungement of the data from these systems. This process can not be determined in advance of knowing the details of these systems.

Audit and system logs will assist in tracking potential elements of the Breach Data.

Additional Long-Term Considerations

(Optional) Impact Assessment Mapping

Identify all instances where the compromised data has been used or accessed post-departure of the defendants to understand the full impact of the breach.

(Optional) Periodic Review and Adjustment

Regularly review the effectiveness of the remediation measures and adjust as necessary to address new security challenges and ensure the integrity of union membership data.

Return, after some interval, to ensure that the Breach Data has not been re-engaged by the Parties Holding the Breach Data.

Conclusions

This remediation plan is designed to not only recover and secure the Local 75's Breach Data but also to restore trust among union members by demonstrating a commitment to protecting their information.

This comprehensive approach addresses both immediate concerns and long-term data security, ensuring compliance with legal standards and fostering a secure data environment.

Yours truly,

ellwood evidence Inc.

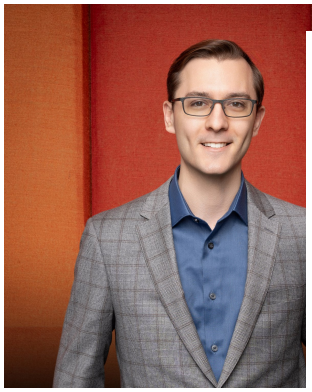
Per:

William B. Ellwood
Senior Investigator

Appendix A – Resume of William B. Ellwood

12

A409



William Ellwood

Forensic Lead,

CISO

CISSP, EnCE

CCPA

(416) 410-1441

William is the Forensic Lead and Chief Information Security Officer for ellwood Evidence Inc., a digital forensic and incident response consultancy. He works with firms to improve their security posture, and to identify, isolate and remediate cyber-threats. Through their work with law enforcement, regulatory agencies and criminal defense firms, he has provided insight into the technical aspects of online fraud and cyber-theft.

With fifteen years of experience in information technology, ediscovery, digital forensics and digital security, William has implemented and investigated a wide range of technologies as they apply to legal matters. He holds a Bachelors of Science in Computational Cognition from Trinity College, University of Toronto. He is a Certified Information System Security Professional and Ontario-licensed Private Investigator.

Court Appearances

on consent, R.D. v. Her Majesty the Queen 2022, before Chief Justice Weibe, Provincial Court of Manitoba, for the Winnipeg Police Service as an expert in:

- the search of materials, including digital and internet based materials, servers and other technological devices including laptops, iPads, digital cameras and USB sticks
- data retrieval, isolation, preservation and destruction processes once material is seized

A409

13

A410

Conferences & Seminars

PANELIST

The Osgoode Certificate in E-Discovery, Information Governance and Privacy

Feb. 22, 2023 ·

Osgoode Professional Development

Created and taught the Collection, Preservation and Processing material as faculty for the Osgoode certificate program.

Disclosure and Detention of Things Seized, Section 490 CC

Oct. 14, 2022 ·

2022 Tech Crimes and Electronic Evidence Symposium

Section 490C of the criminal code addresses the requirements surrounding return of seized items. We explore the issues which may arise when seized items are repositories of digital data.

Protecting your Business/Workplace from Fraud

Oct. 12, 2022 ·

25th Annual Fraud and Anti-Counterfeiting Conference

From preventing phishing to ensuring online safety and physical safety within your office/home office premises, education of staff to protect against fraudsters.

E-Discovery, Information Governance and

Advancing the Industry

PAPERS

Sedona Canada - Sedona Canada Commentary on Discovery of Social Media

Feb. 1, 2022

Forthcoming. My primary contribution was updating and revising the sections on ephemeral messaging, preservation and presentation.

Sedona Canada - Commentary on Privacy and Information Security for Legal Service Providers: Principles and Guidelines

May 23, 2019

In this commentary, the Sedona Canada working group on Privacy and Information Security attempted to make the nitty-gritty of information security as approachable as possible, with practical tips for securing law-firms large and small.

TEACHING

Osgoode Professional Development, 2019 - Present

Teaching the *Collection, Preservation and Processing* section in the Osgoode Certificate in E-Discovery, Information

A410

14

A411

Privacy: Data Preservation & Processing

Sep. 22, 2021 ·

Osgoode Hall Professional Development

Presented developments in In-Place Data Search, Litigation Holds and modern document processing and analytics solutions as part of The Osgoode Certificate in E-Discovery, Information Governance and Privacy.

The New Balancing Act: Staying Cyber-Safe Wherever You Are

Apr. 1, 2021 ·

Intellectual Property Institute of Canada

An overview of key challenges and unique security threats associated with remote access and adopting best practices to protect small ad mid-sized firms (and their clients) against fraudsters. Checklists and worksheets provided to kickstart security programs.

Governance and Privacy. Regular panelist and presenter.

Guidance Software Part-Time Trainer, 2014 - 2018

Instructed the EnCE Preparation Class at Guidance's Dulles Virginia facility. Regularly facilitated virtual classroom instruction. Graded EnCE examinations.

COMMITTEES

The Sedona Conference - Working Group 7

Apr. 10, 2019

The mission of Working Group 7 is to create forward-looking principles and best practice recommendations for lawyers, courts, businesses, and others who regularly confront e-discovery issues in Canada.

A411

15

A412

ATTENDEE

EnFuse 2019

Nov. 12, 2019

Bringing together thought-leaders in cybersecurity, digital investigations, AI and eDiscovery to discuss best practices, Enfuse 2019 offered more than 100 breakout sessions and hands-on technical labs.

The Investigators' Guide to Testifying in Non-Criminal Legal Proceedings

Apr. 17, 2019

A comprehensive overview of all the key steps that go into giving effective testimony. An experiential learning day with numerous opportunities to practice testimony and individualized feedback from experienced counsel.

12th National Symposium on Tech Crime and Electronic Evidence

Jan. 25, 2019

Disseminating information and techniques to more effectively investigate, prosecute, defend or adjudicate technology and internet crimes.

Blackhat 2017

Jul. 26, 2017

Black Hat is the world’s leading information security event, providing attendees with the very latest in research, development and trends.

Computer and Enterprise Investigations Conference 2014

May 19, 2014

CEIC brings together security, e-discovery and forensic investigation professionals for in-depth discussions on security with industry experts representing leading government agencies and corporations from around the world.

A412

16

A413

Computer and Enterprise Investigations Conference 2013

May 20, 2013

CEIC is one of the largest international gatherings with a focus on the latest developments in cybersecurity, digital investigations and e-discovery.

A413

17

A414

Certifications & Professional Education

A414

18

A415

DIGITAL FORENSICS

Cellebrite Certified Physical Analyst

Jul. 14, 2023

The Cellebrite Certified Physical Analyst (CCPA) course is a 3-day advanced level program designed for technically savvy investigators, digital evidence analysts and forensic practitioners. Physical Analyzer software will be used extensively to explore recovered deleted data, database contents, advanced search and analysis techniques, verification and validation, and reporting.

Cellebrite Certified Operator

May 10, 2023

The CCO is a 2-day intermediate level certification program which is designed to teach with extracting data in a forensically sound manner using UFED Touch or UFED 4PC. It aims to teach digital forensic examiners data extraction techniques across a variety of devices.

Nuix Workstation Discovery Core

Apr. 26, 2023

The foundational knowledge for effective use of Nuix Workstation, to create cases, data process, search and review content.

EDISCOVERY

Certified EDT Site Administrator (CESA)

Sep. 18, 2018

the most comprehensive of EDT's certifications, CESA includes all other EDT training content for those responsible for administration of the entire EDT environment.

Relativity Certified Administrator 8.3

Feb. 21, 2016

The Relativity Certified Administrator (RCA) program ensures that case administrators fully understand Relativity's capabilities, allowing you to maximize the software's flexibility and provide an intuitive interface for end users.

EnCase Certified eDiscovery Practitioner (EnCEP)

Mar. 18, 2014

The EnCase® Certified eDiscovery Practitioner(EnCEP®) program certifies private and public sector professionals in the use of Guidance Software's EnCase® eDiscovery software as well as their proficiency in e-discovery planning, project management, and best practices, spanning legal hold to load file creation. EnCase eDiscovery is the leading e-discovery solution for the search, collection, preservation, and processing of electronically stored information(ESI). Earning the EnCEP certification illustrates that a practitioner is skilled in the application of the solution to manage and successfully complete all sizes of e-

A415

19

A416

Certified Forensic Security Responder (CFSR) [In Progress]

Nov. 21, 2019

The CFSR certification acknowledges professionals who have mastered the necessary skills to prepare for cyber-attacks, perform attack detection, validate and prioritize alerts and contain cyber incidents. In addition, it demonstrates the professional's ability to conduct root cause analysis, manage a cyber breach remediation process, and evaluate lesson learned.

Certified Information Systems Security Professional (CISSP)

Dec. 28, 2018

The CISSP is a rigorous, vendor-neutral program that demonstrates competence across eight IT security domains. It is the NSA's certification baseline for information security and policy management.

Passware Kit Forensic Certification

Aug. 22, 2014

... apply Passware in different scenarios, to include, encrypted files, email passwords, Windows passwords, Apple passwords, encrypted volumes and more.

EnCase Certified Examiner (EnCE)

Aug. 9, 2012

The EnCase® Certified Examiner(EnCE®) program certifies both public and private sector professionals in the use of Guidance Software's EnCase computer forensic software. EnCE certification acknowledges that professionals have mastered computer investigation

discovery matters in accordance with the Federal Rules of Civil Procedure.

A416

20

A417

methodology as well as the use of EnCase software during complex computer examinations. Recognized by both the law enforcement and corporate communities as a symbol of in-depth computer forensics knowledge, EnCE certification illustrates that an investigator is a skilled computer examiner.

FORENSICS TRAINING

Cellebrite

Cellebrite Certified Physical Analyst (CCPA)
Cellebrite Certified Operator (CCO)

Sumuri / Passware

Surviving Encryption

Guidance Software

EnCase eDiscovery
EnCase CyberSecurity
EnCase Enterprise
Network Intrusion Investigations
Advanced Internet Investigations
Advanced Computer Forensics
Computer Forensics II
Computer Forensics I

EDISCOVERY TRAINING

kCura

Relativity Analytics
Relativity Infrastructure
Relativity Processing
Relativity Assisted Review

edt.

edt Platform Administration

A417

21

A418

Experience & Education

PROFESSIONAL EXPERIENCE

ellwood Evidence Inc.
Forensic Lead, CISO (2018 - present)
Senior Examiner (2013 - 2018)
Forensic Examiner (2011 - 2013)

Guidance Software
Part-Time Forensic Trainer (2014-2018)

ellwood Associates Inc.
Solutions Architect (2011-2013)
Support Administrator (2009-2011)

EDUCATION

University of Toronto, Trinity College
Bachelor of Science, Computational Cognition (2012-2017)

A418