Dear Survivor,

I am writing to you with important information about a recent data loss that could potentially lead to a privacy breach involving your personal information as a current or previous client accessing our services.

In this letter we:

- explain what happened;
- explain the way we hold personal information at Salal;
- tell you what the data breach could mean for your privacy;
- give you our assessment of the risk;
- tell you steps we have taken to mitigate the risk and prevent any occurrences
- tell you what steps you can take to minimize the risk.

What Happened

At about 3:30 am on December 3rd, 2023, our new (under construction) office site was broken into, and technology hardware required for service delivery and operations was stolen. One of the hardware items that was stolen was a copy of our back-up server. This was **not** a "data hack". Just because the person who stole it has the hardware, doesn't mean that they know what to do with it. Moderate to high knowledge and IT skills of how to route the information and find it in the drive would be required to access any information held on the drive.

We do not believe that this break-in was targeted to destabilize Salal SVSC or the survivors that we serve.

How is your information held at Salal?

Your client file, with information about your sessions, medical information, etc, is not held at Salal at all. It is held by a program called Jane which is a third-party platform that has nothing to do with Salal. The Jane platform is "encrypted" which means that unless someone has the passwords to get in, they cannot access that data. None of your file(s) is able to be accessed because of this data loss and potential breach.

We do have a file on our server which has waitlist information or client contact information, including your email and phone number, police file number, any safety concerns, and what services you have been requesting.

But getting to those files on the server that was stolen is what requires sophisticated understanding of computer software and how to hack in.

What the data breach could mean for you personally

It is possible that your name, email address, telephone numbers, and notes about safety risks or what services you have requested, could be released, sold, and shared publicly.

Do we think your data will be found and used?

We think it is a low possibility that the thief will be able to get into the computer equipment they have stolen and get access to the particular file that has your identifying information on it, yet that doesn't change the risk to your privacy which we take very seriously.

We have conducted a privacy impact assessment on the incident and it may be that the risk to your privacy is moderate. We are of course very concerned with ANY possible data breach, even if the possibility is moderate, and we are doing everything we can to make sure that this cannot happen again.

What steps have we taken?

Since December 3rd we have taken the following steps to increase the security to our space and our data.

- Made a police report
- Alerted our landlord at the City of Vancouver and other tenants in the building
- Reviewed security camera footage to identify the person that gained access to our space
- Have added cameras to the space and specifically focused on our IT room
- Reinforced all access points with additional layers of security (metal plates over the locks and reprogramming of all FOBs that can access our space)
- Migrated our back-up server to an encrypted cloud server
- Created an internal plan to add additional layers of safety to our server (encryption and password protection)
- Are in process of communicating with all stakeholders impacted by the data loss

What steps can you take?

There are a few things that you can do at your end to increase your protection from potential harm.

- Change all your passwords for accounts that hold sensitive information (banking, CRA, email account that you used at Salal)
- Install a "two factor identification authentication" on any accounts you have that use your email. If you don't know how to do that, you can either google it, or go to a public library where they can help you.
- Use websites like https://haveibeenpwned.com/ to see if your email shows up as one that has been compromised in a data breach; this will cover any data breach your email has been involved in. If your email has been part of a breach it doesn't necessarily mean it is from this incident.
- Be alert from any spam or phishing emails that seems to come from Salal. A "phishing email" is one that looks to come from a reputable email address, and asks you for personal information. Check the sender's address, regardless of the name of the sender, to make sure it is a Salal address. If you have any doubt, call Salal and ask if they sent the email. Don't send personal information (eg your birthdate, credit card number, etc) in response to such an email. **Salal will never ask for that information by email or text.**

We know this can have a big impact

We want to acknowledge and affirm the distressing nature of this news for survivors, and our community. We know that violations of safety, transgressions against our autonomy, and invasions of privacy can be triggering. In addition to our accountability for this breach, we offer our full support of survivors who may be navigating overwhelming emotions because of it.

24-Hour Crisis & Information Line: 1-877-392-7583
Salal Connect Text and Chat Support: 604-245-2425 | salalsvsc.ca/connect-chat/

The Salal team is available for you to call us with questions and concerns about the loss of your personal information. **You may call 604-255-6228 9:00AM - 5:00PM, Monday-Friday with any questions you have, or email admin@salalsvsc.ca**

We have also established a section on our website https://www.salalsvsc.ca/securityrecommedations/ with updated information and links to resources that offer information on what to do if your personal information has been compromised.

We take our role in safeguarding your personal information and using it in an appropriate manner very seriously. Please rest assured that we are doing everything we can to increase safety for the future, enhance security at our new space, and ensure the privacy and protection of our clients, donors, community members and staff.

Please note that under the Personal Information Protection Act (PIPA) you are entitled to file a complaint with the Office of the Privacy Commissioner of British Columbia with regard to this breach. Complaints may be forwarded by email: info@oipc.bc.ca or by mail to:

Office of the Information and Privacy Commissioner for British Columbia

PO Box 9038 Stn. Prov. Govt. Victoria B.C. V8W 9A4

Additional information is available on the Privacy Commissioner's website at https://www.oipc.bc.ca/

Having our new office space broken into, and this theft occurring has been devastating and we want you to know that we are doing everything required to ensure the safety of our space. We want to reiterate this poses a moderate risk to you as a current or past survivor accessing our services. Should you have any questions regarding this notice or if you would like more information, please do not hesitate to communicate with the undersigned.

Sincerely,

Dalya Israel (she/her)
Executive Director
Salal Sexual Violence Support Centre (Formerly WAVAW Rape Crisis Centre)
admin@salalsvsc.ca