Dear Donor,

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 donor.

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

About 3:30 am 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?

As a donor your tax receipt information is kept on our server along with back-up images of cheques that have been deposited, for our audit. We do not keep debit or credit card information on our server.

What the data breach could me for you personally

As a donor, it is possible that your name, address, phone number and banking information could be released, sold, and shared publicly if you have donated to us by **cheque**. **No credit card or debit card information has been compromised through this loss**. If you donate online with us, your banking information is safe, Salal does not store this information on our server, and your financial security is not at risk.

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

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 had a "privacy risk assessment" done by Privacy Expert, Mayowa Abisoye at Overholt Law, and we are told 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. We have been working at reinforcing all access points, we have alerted VPD and our landlord at the City of Vancouver, and have installed cameras in the space to specifically safeguard our server and IT room.

What steps can you take?

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

- Steps you can take as an individual to increase protection from potential harm from the breach are to change all your passwords for accounts that hold sensitive information (banking, CRA, email account that you used at Salal), install a two factor authentication on your bank accounts and CRA account
- 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.
- You should remain vigilant about suspicious activity and check your credit reports, as well as your other account statements, periodically over the next 12 to 36 months. You should immediately report any suspicious activity to the credit bureaus.
- Salal is working closely with Vancouver Community Network (VCN), our contracted, third party tech company to investigate the full scope of the data loss and support us to be even more well-secured should we encounter another break-in and are additionally migrating our data to an encrypted cloud server.
- Please be on alert for spamming for phishing emails or text messages from our organization. **We will never ask for personal or banking information over email or text**. If you are unsure if the email you have received is authentic, please call our office line.

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, including you. 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, we want to reiterate this poses a moderate risk to you as a current or past independent contractor supporting our programs and 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)