Safeguarding Against Digital Financial Abuse When Opening a New Bank Account

Survivors of financial abuse may decide to open a new bank account online or in person, either before or after leaving a violent relationship.

This information sheet provides some guidance for survivors to protect against further digital financial abuse when opening a new account.

Changes to an Existing Bank Account: Accidently Alerting an Abuser

Making changes to improve the security or privacy of an existing bank account may tip off an abuser, potentially escalating their abuse. Abusers may:

- Receive email or text notifications when changes are made to accounts they have shared access to.
- Receive calls from bank staff confirming changes to accounts they have shared access to.
- Be using stalkerware to track the activity on the survivor's devices to see what websites or apps are being accessed.
- Have the survivor's banking and password information, allowing them to log in from their own device and notice if an existing password no longer works.

If a survivor suspects any of these, they may want to open a new bank account without closing the account the abuser has access to.

Safety Considerations when Opening a New Account

Survivors may want to contact a local shelter or anti-violence organization to discuss their options and develop a safety plan before opening a new bank account.

This can be especially important when any of the following is occurring:

- **The abuser is withholding ID to prevent the survivor from opening an account**. Shelters or transition houses can support an application for

temporary ID or assist with recommendations for banks that will open accounts for survivors without ID.

- **The abuser has placed** location tracking devices on the survivor's car or a Bluetooth tracker (e.g. airTag) or spyware on the survivor's device to trace where they go when trying to go to the bank.
- Spyware **has been downloaded on the survivor's device** that allows the abuser to see what the survivor is doing, including when they open a new bank account online and their login and password information.

Opening an account online:

- If opening a bank account online through an app or website, use a safe device that the abuser is not monitoring, such as the device of a trusted friend or family member or one at work or the local library.
- Log out of online banking on the computer/device you are using, especially if it is a shared or public computer.
- Use a secure, private Wi-Fi network. Avoid using public Wi-Fi for sensitive actions like opening a bank account.
- If public Wi-Fi must be used, consider accessing your accounts via a VPN (Virtual Private Network) to help protect your data.
- Clear Internet search browser history or open the account in a private browser if an abuser still has access to family devices.
- If you need to input an email address, phone number, or other contact information, use accounts that the abuser does not have access to. You may need to open a new email account for your banking communication, especially if updates for the new account are sent to an existing email address that the abuser monitors, as this will alert him that you have opened a new account.

Opening an account in person:

- If your location is being tracked, consider parking the vehicle farther from the bank and/or leaving your compromised device in the car if it's safe to do so.

General Safety Tips

- Use a password that uses a mix of upper and lowercase letters, numbers, and special characters.
- Do not reuse passwords or PINs from other accounts; better yet, use a password manager to store them securely.
- Choose a bank that offers two-factor authentication (2FA) and enable it. This adds an extra layer of security by requiring a second kind of verification, such as a code sent to a phone number or email. When setting this up, make sure the email or phone you use for verification is one that the abuser does not have access to.
- Do not put anyone else's name on the account or give anyone access.
- Set up notifications to an account not being monitored for all transactions or attempted logins so you will be aware if there is any suspicious activity or unauthorized access.
- Check the privacy settings to see who has access to your info (online or when setting up the account at the branch).
- Make sure the answers to your security questions are not info the abuser knows.
- If you are still sharing space with the abuser, keep debit/credit cards associated with your new accounts/banks elsewhere/hidden.

- Consider using a different bank or being very clear with your existing bank that you want there to be no connections between your existing accounts and this account. For example, if you open a new account at your existing bank, it may show up on your online banking's account list with your other accounts, which could link to an abuser's online account.
- Exercise caution if moving money from an existing account the abuser can access to your new account, as they may be able to tell from the statements/transactions that you have a new account and which institution it's at.
- Be careful about updating your credit card or banking info in other apps/platforms; if you add your new information to an account the abuser can access, he will then see your new banking info.

These precautions can help protect your new bank account from being misused by an abuser. If you need support, contact a local shelter and/or check out our information sheet, 6 Tips for Securing Your Online Financial Information, for guidance on staying safe.

Technology-Facilitated Gender-Based Violence (TFGBV) is part of a continuum of violence that can be both online and in-person. If you or someone you know is experiencing TFGBV, you are not alone. You can use sheltersafe.ca to find a shelter/transition house near you to discuss options and create a safety plan. You don't need to stay in a shelter to access free, confidential services and support. For more information about digital financial abuse, see our full Digital Financial Abuse Toolkit.

This project was funded by TD Bank Group, through its corporate citizenship platform, the TD Ready Commitment.