Privacy Guide

Agronomy Company of Canada ("Agromart") and Sollio Agriculture LP ("Sollio AG") are pleased to advise that a settlement has been reached in a class action related to a security breach that occurred in 2020 arising out of a cyberattack.

For more information on the settlement, please visit:

https://www.foremancompany.com/agromart-sollio-privacy-breach or

https://waddellphillips.ca/class-actions/sollio-ag-and-agromart-class-action/

Agromart and Sollio AG take this opportunity to remind you about the importance of data security in Canada's agricultural sector and to share some lessons learned and improvements that have been made recently to make our systems more secure.

Electronic Security and Privacy in Canada's Agricultural Sector

Privacy and data security is a growing priority for all industries. All organizations, large and small, have a role to play in ensuring that the devices and data they use to perform their work are secure. Most importantly, strong privacy and data security practices foster a sense of trust between organizations and individuals who share their information with them.

Privacy and data security are especially important for the agricultural sector, which has seen a steep increase in the adoption of connected technology in recent years. From smartphones, to farm management software, to GPS-guided and connected farm equipment, the entire agricultural industry relies on forms of internet-enabled or connected systems. It is crucial that everyone in the agricultural sector use devices and systems safely, and ensures that that the devices and systems have appropriate safeguards in place so that the users remain as safe as possible. Further, like all other equipment, connected devices and systems should be appropriately maintained, and their security systems and safety measures should be checked regularly and kept up to date.

If devices and systems become outdated or are not properly maintained or secured, they become prime targets for criminals looking to perpetrate cyber attacks. Cyber attacks can take many forms. In recent years, they have become more destructive: in many cases, criminals have made computers and devices inoperable, sometimes to the point where businesses have been unable to function at all. In the worst of cases, criminals steal data and then lock organizations out of their computer systems and devices, and then demand a ransom to delete the data and unlock the computers and devices. These ransoms are

often substantial: Between 2021 and 2022, the average ransom doubled to over $1.5 million. This can happen to large organizations, but also to small businesses.

In all cases, cybersecurity incidents that have attacked businesses are costly and time-consuming to address, and can be very expensive to get systems and data restored. In the agriculture industry, this can also lead to broader food security concerns. There are reports of cyber security incidents that appear to involve forms of market espionage. Canada is among the largest agricultural producers and exporters in the world. Our market is valuable, and we all have a role to play in protecting the data and information within Canada's agricultural sector.

How do criminals attack organizations?

Criminals can attack organizations in a few different ways:

Business email compromise: A business email compromise occurs when a criminal gains access to a victim's email account, often to steal sensitive information stored in the account or to trick the user into redirecting funds to the criminal's bank account (usually by impersonating a vendor or other payee). Criminals often compromise email accounts by sending the user a phishing email. A phishing email is one that may appear legitimate, but will contain a hyperlink or QR code that directs the user to a webpage asking the user to input their credentials. A criminal can also use its access to the user's email account to send further phishing emails from it, in an attempt to get others to expose their credentials (called "lateral phishing").

Be careful in opening emails from unknown senders, or emails that are asking you to open a link or click on a document. While an email may look like it is coming from a legitimate source, you should check the email address, which you can do by hovering your cursor over the address. If the sender's email is unfamiliar, be wary. Typographical errors, or unusual sentence structure are also red flags for phishing.

Exploiting vulnerabilities in a system or device: Criminals can also gain access to computer systems and connected devices by exploiting vulnerabilities in the system or device. While manufacturers and software developers will work to ensure their systems meet certain minimum security standards, they often discover vulnerabilities after their products are released. To address these vulnerabilities, they issue "patches" which users can download and install before criminals attack their unpatched system. In rarer cases, the criminals will discover and exploit new vulnerabilities before either the manufacturer or software developer (or the general public) knows about it. These are called "zero-day" vulnerabilities. It is therefore important to update your software to incorporate current patches, when they become available. Again, older devices and software systems often present a unique level vulnerability, particularly if there is a risk that patches or updates

have not been regularly performed. Sophisticated hackers understand this risk and use it to their advantage.

Ransomware: Phishing emails/business email compromises and unsecured devices can also be used to deliver malicious software to a user's computer or other devices, leading to a second common type of attack called **ransomware**. Ransomware is a malicious software that locks ("encrypts") a user's files or systems. Ransomware can be delivered in numerous ways, including by a phishing email or through a compromised user account, or, less commonly, through USB keys. Prior to deploying ransomware, the hackers will often steal data and/or delete data backups. As mentioned above, ransomware syndicates will demand a ransom in exchange for deleting the stolen data and unlocking ("decrypting") files or systems.

How do Sollio AG and Agromart protect your information?

The security measures that Sollio AG and Agromart, and every member of the agriculture sector, implements are crucial to keeping everyone and their information safe. Sollio AG and Agromart have implemented the following types of security measures to minimize the risk to the data that you share with it:

- Designated a Privacy Officer to provide leadership and accountability with respect to privacy and security policies and practices within our organizations;
- Deployed multifactor authentication for all external services and internal administrative services;
- Moved all infrastructure to a cloud service, protected by multifactor authentication and conditional access;
- Ensured that each company site is on its own network;
- Implemented an enterprise password manager and strengthen the password policy;
- Deployed a new generation of anti-virus/EDR platform and reviewed firewall configuration;
- Implemented a Data Lost Prevention (DLP) service to protect against data exfiltration and enhance the control to critical files and databases;
- Implemented alerts for administrator accounts, including alerts for failed login and unusual activities; and
- Provided training and awareness campaigns on cybersecurity.

What can your farming business and individuals do to help prevent cyber attacks?

It is important that all organizations take privacy and data security seriously. We have set out some tips below to help you ensure that your privacy and data security practices are strong, and you are protected from cyber criminals:

- **Use tried-and-true security measures:** Measures like strong passwords that are changed regularly, password managers, and multi-factor authentication will go a long way toward securing your data. Combining these measures with other common data security steps like keeping software updated, encrypting stored and delivered sensitive data, and using malware monitoring software (such as "endpoint detection and response") will help thwart many cybersecurity risks.

  A strong password will have a combination of upper and lower case letters, numbers and symbols. It can be a word or phrase that only you would know, that includes changing numbers for letters, such as "R0verismyd0g^".

- **Invest in cybersecurity training**: Unfortunately, human error is one of the most common cybersecurity risks that everyone faces. Investing in training that addresses common risks like phishing and ransomware is important. Free training programs are available online, such as one offered by the Government of Canada at: https://www.cyber.gc.ca/en/education-community/learning-hub/courses/625-cyber-security-small-medium-organizations

- **Decommission devices and accounts that are no longer needed**: Old, or unmonitored devices and accounts that are no longer receiving security updates can provide hackers with easy access to your system. Consider routinely updating and/or decommissioning these devices and accounts.

- **Keep backups of data, including disconnected or immutable backups**: If you are the victim of an attack, having secure, recent backups is an important step to making sure that your organization can get back up and running quickly.

- **Segment your network**: If your organization must use devices that are not secure, consult IT professionals about segmenting your network to ensure that your critical systems do not interact with the unsecure devices.

- **Consult experts**: If you are uncertain of what steps to take or how to secure your systems, consult IT security experts. They will be able to help you implement data security measures that are appropriate for your systems.

Where can I learn more about cybersecurity?

More information about privacy and data security practices can be found at:

Canadian Anti-Fraud Centre, *Protect yourself from scams and fraud*: https://www.antifraudcentre-centreantifraude.ca/protect-protegez-eng.htm.

Community Safety Knowledge Alliance, *Cyber Security Capacity in Canadian Agriculture*: https://cskacanada.ca/projects/strengthening-the-cyber-security-capacity-of-canadas-agricultural-sector/.

Government of Canada (Agriculture and Agri-Food Canada), Cyber security and your farming business: https://agriculture.canada.ca/en/programs/tools-manage-farm-risk-and-finance/cyber-security-and-your-farming-business.

Ali Dehgnantanha, Hadis Karimipour, Amin Azmoodeh, *Cybersecurity in Smart Farming: Canada Market Research*: https://arxiv.org/abs/2104.05183

Dr. Taylor Reynolds (Massachusetts Institute of Technology, Internet Policy Research initiative) *Cybersecurity for Agriculture*: https://www.usda.gov/sites/default/files/documents/S22_Taylor_Connectivity-in-Rural-America.pdf