Denro
Property Management Ltd.

2370 - 2nd Avenue
Regina, Saskatchewan
Canada S4R 1A6
Phone: (306) 586-1501
Fax: (306) 586-0015
www.denro.ca

Notification of Security Incident

What happened?

We are writing to inform you that one or more of our user accounts was accessed by an unknown and unauthorized third party. This may have led to a potential compromise of your information.

On March 16, 2022, we discovered that our computer systems experienced a cyber attack. We immediately engaged our IT provider, PC Place, to secure and restore our systems. This included their specialists identifying the breached accounts, wiping out and ultimately replacing compromised workstations, reviewing server logs and activity and resetting all security credentials and passwords.

We have not found any proof that your personal information was accessed or copied. However, we cannot rule out the possibility that an unauthorized third party obtained your personal information. As a result, we are writing to advise you now that it is possible that any personal information provided to us in the past could be compromised. This includes:

- Your full name
- Address and contact information (e.g., your mailing address, telephone number and email address)

Response and Steps Taken To-Date to Protect You

We take the safety and security of your personal information very seriously and we are taking steps to protect you.

As soon as we became aware of this incident, we were in immediate contact with the Regina City Police and RCMP National Cyber Crime Coordination Units. We took our systems offline, changed all passwords, purchased replacement hardware and added multi factor authentication to all email and remote login accounts.

We will also be reporting this incident to the Office of the Privacy Commissioner of Canada.

Steps to Protect Yourself

We have no reason to believe that the unauthorized third party had any specific interest in your personal information. However, as a general precaution to protect your personal information, we recommend that you follow the steps outlined below to help reduce potential risks.

1. Be vigilant for signs of identity fraud.

It is possible that the unauthorized third party or others could attempt to use the personal information listed above for the purposes of attempted identity fraud. This means that they could try to use that information to impersonate you to obtain a benefit or service. Please remain vigilant for any potential signs of identity

fraud, such as suspicious activity on your bank accounts, unauthorized redirection of mail, unauthorized porting of your mobile phone, or receiving goods or services that you did not order.

2. Be wary of social engineering attempts

In cases of identify fraud, sometimes a fraudster may contact you to trick you into providing more personal information or access credentials. To protect yourself against social engineering:

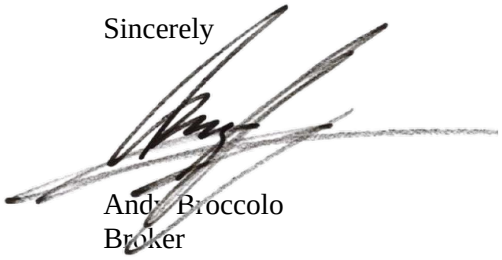
- be wary of anyone that contacts you and requests personal information or access credentials from you, even if they appear to know other details about you.
- do not respond to email or text messages asking for personal information – few legitimate organizations will ask for personal information by email or text;
- be careful of unsolicited telephone calls which purport to be from a government authority or business; and
- remain vigilant regarding any suspicious emails that ask you to open attachments or click on links.

Our Commitment to You

We take the security of your personal information very seriously. We apologize for any inconvenience this may cause you. We want to reassure you that we continue to work very hard to make sure your personal information is protected.

We understand that you may still have questions and concerns regarding this matter. If you do, please do contact us.

Sincerely



Andy Broccolo
Broker