Office of the Information and
Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	WFG Dealer Connect, as reported by WFG Securities Inc. (Organization)
Decision number (file number)	P2019-ND-084 (File #009921)
Date notice received by OIPC	October 3, 2018
Date Organization last provided information	May 23, 2019
Date of decision	June 25, 2019
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify this individual pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • telephone number, • signature, • date of birth, • Social Insurance Number, • investment account number, and • banking information. This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On September 19, 2018, a trade document containing a client's personal information along with redemption instructions was sent by fax from an advisor's branch office in Alberta to the Organization.

	• The document was intercepted at some point and the banking information initially provided was replaced and submitted directly to the fund company by fax for processing. This was an attempt to redirect funds to an unknown third party's account with another bank. • The breach was discovered on September 20, 2018, by an employee during the course of a transaction review. • The client confirmed the account was not his, which led the Organization to believe that the funds may have been misappropriated. • The Organization is unable to determine at what point the interception occurred. • An investigation determined that no employees of the Organization were involved in the misappropriation of the information/funds.
Affected individuals	The incident affected one (1) individual residing in Alberta
Steps taken to reduce risk of harm to individuals	• Stopped the redemption request to prevent any further harm to the affected individual. • Reported the incident to law enforcement. • Escalated the incident to the product providers. • Heightened the review of similar transactions and working with the back office and local authorities to fully identify the cause of the breach. The client was reimbursed any losses incurred.
Steps taken to notify individuals of the incident	The affected individual was notified by letter on October 3, 2018.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to affected individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.	The Organization reported the possible harms that might result from this incident include "The client's funds may be re-directed to an unknown third party not affiliated with his account in any way" and "The client's personal information could be used to create a false identity." I agree with the Organization's assessment. The financial and identity information at issue could be used to cause the harms of fraud, identity theft and financial loss. These are significant harms.

Real Risk The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.	The Organization reported that the "Amount information [sic] was misappropriated to an unknown entity. We are working with the product providers to ensure that any losses from the account are returned to the client." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate interception and misappropriation). There is no way to confirm the unauthorized party did not access or copy the information in some form.

DECISION UNDER SECTION 37.1(1) OF PIPA

Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individual.

The financial and identity information at issue could be used to cause the harms of fraud, identity theft and financial loss. These are significant harms. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate interception and misappropriation). There is no way to confirm the unauthorized party did not access or copy the information in some form.

I require the Organization to notify the affected individual in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individual in a letter dated October 3, 2018 in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner