

Information and Privacy Commissioner,  
Ontario, Canada



Commissaire à l'information et à la protection de la vie privée,  
Ontario, Canada

---

## ORDER MO-4546

Appeal MA23-00475

Toronto Police Services Board

July 12, 2024

**Summary:** The appellant was the victim of fraud, losing a large amount of money when he transferred Bitcoin to another individual under false pretences. The police conducted an investigation but did not have enough information to proceed with criminal charges. The appellant received an occurrence report under the *Act* with an individual's information withheld under section 14(1) (personal privacy). He appealed the police's access decision, stating that he required this information to recover the lost money.

In this order, the adjudicator finds that the information is exempt from disclosure under section 38(b) (personal privacy, with the report containing the appellant's personal information). He finds that the extent, if any, of the individual's involvement in the crime is not known, favouring withholding the information. Additionally, he finds that the appellant has not adequately explained how the information at issue would assist with recovering the lost money. He upholds the police's decision.

**Statutes Considered:** *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56, as amended, sections 2(1) (definition of personal information) and 38(b).

**Orders Considered:** Orders M-655, PO-2236, MO-1664, MO-3370, MO-4500, MO-4503, P-602, and 151.

### OVERVIEW:

[1] The requester was the victim of fraud, losing a large amount of money when he transferred Bitcoin to another individual under false pretences. He submitted the following

request to the Toronto Police Services Board (the police) under the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*):

“I need a copy of the Binance report from [named individual] which should be attached to the previous police report that was already made ...”

[2] The police issued a decision granting partial access to an occurrence report, with portions of the report withheld under section 14(1) (personal privacy). The police also issued a supplementary decision stating that they had a copy of the Binance transfer report<sup>1</sup> in their possession, but it was not in their custody or control for the purposes of the *Act*.

[3] The requester (now the appellant) appealed the decision to the Information and Privacy Commissioner of Ontario (IPC). During mediation, the appellant explained that he is seeking the individual’s name in the police report to assist with recovering his lost funds, referring to the incident that led to him initially contacting the police. He stated that he is not appealing the police’s decision that the Binance report is not in their custody or control. The police confirmed that they are maintaining their decision to refuse access to the withheld information in the occurrence report. During mediation, the police stated that they were unable to notify the individual as their contact information was not known.

[4] No further mediation was possible, and the appeal was transferred to the adjudication stage of the appeal process, where an adjudicator may conduct an inquiry. I reviewed the record at issue and determined that it appeared to contain the appellant’s personal information and accordingly I added the application of section 38(b) of the *Act* (personal privacy) as an issue in the appeal. I conducted an inquiry where I sought and received representations from the police and the appellant. Representations were shared in accordance with the IPC’s *Code of Procedure*.

[5] For the reasons that follow, I uphold the police’s decision to withhold the individual’s personal information.

## **RECORDS:**

[6] The record at issue is an occurrence report with the name, sex, and date of birth of an individual withheld (the report).

---

<sup>1</sup> Binance is a cryptocurrency exchange, and the transfer report identifies who accessed money associated with a particular wallet.

## **ISSUES:**

- A. Does the report contain “personal information” as defined in section 2(1) and, if so, whose personal information is it?
- B. Does the discretionary personal privacy exemption at section 38(b) apply to the information at issue?

## **DISCUSSION:**

### **Issue A: Does the record contain “personal information” as defined in section 2(1) and, if so, whose personal information is it?**

[7] Before I consider the exemption claimed by the police, I must first determine whether the report contains “personal information” and if so, whether the personal information belongs to the appellant, other identifiable individuals, or both. “Personal information” is defined in section 2(1) of the *Act* as “recorded information about an identifiable individual.”

[8] Information is “about” the individual when it refers to them in their personal capacity, which means that it reveals something of a personal nature about the individual. Information is about an “identifiable individual” if it is reasonable to expect that an individual can be identified from the information either by itself or if combined with other information.<sup>2</sup> Section 2(1) of the *Act* gives a list of examples of personal information.

[9] The parties do not dispute that the report contains the personal information of the appellant and other individuals. The appellant, through his representative, states that the information at issue also contains the Bitcoin wallet address of the individual.

[10] I have reviewed the report and I find that it contains the names and addresses of the appellant and other individuals, which constitute personal information under the *Act*. The individual’s Bitcoin wallet address is not part of the withheld information. Regardless, having found that the report contains the personal information of the appellant and other individuals, I will consider the application of the personal privacy exemption at section 38(b).

### **Issue B: Does the discretionary personal privacy exemption at section 38(b) apply to the information at issue?**

[11] Section 36(1) of the *Act* gives individuals a general right of access to their own personal information held by an institution. Section 38 provides some exemptions from

---

<sup>2</sup> Order PO-1880, upheld on judicial review in *Ontario (Attorney General) v. Pascoe*, [2002] O.J. No. 4300 (C.A.).

this right.

[12] Under section 38(b), where a record contains the personal information of both the appellant and another individual, and disclosure of the information would be an “unjustified invasion” of the other individual’s personal privacy, the institution may refuse to disclose that information to the appellant. This involves a weighing of the appellant’s right of access to their own personal information against the other individual’s right to protection of their privacy.

[13] The section 38(b) exemption is discretionary. This means that the institution can decide to disclose another individual’s personal information to a requester even if doing so would result in an unjustified invasion of the other individual’s personal privacy. If disclosing another individual’s personal information would not be an unjustified invasion of personal privacy, then the information is not exempt under section 38(b). Additionally, the requester’s own personal information, standing alone, cannot be exempt under section 38(b) as its disclosure could not, by definition, be an unjustified invasion of another individual’s personal privacy.<sup>3</sup>

[14] Sections 14(1) to (4) provide guidance in determining whether disclosure would be an unjustified invasion of personal privacy under section 38(b). If any of the five exceptions in sections 14(1)(a) to (e) apply, the section 38(b) exemption does not apply to the report. Section 14(4) sets out certain types of information whose disclosure is not an unjustified invasion of personal privacy. None of the parties provided representations on the section 14(1) exceptions or the section 14(4) situations, and based on my review of the information at issue they are not relevant to the appeal.

[15] Section 14(2) provides a list of factors for the police to consider in making this determination, while section 14(3) lists the types of information whose disclosure is presumed to constitute an unjustified invasion of personal privacy. In their representations, the police and appellant have relied on or discussed the presumption in section 14(3)(b) and the factors in section 14(2)(a), (b), (d), (h), and (i):

(3) A disclosure of personal information is presumed to constitute an unjustified invasion of personal privacy where the personal information,

(b) was compiled and is identifiable as part of an investigation into a possible violation of law, except to the extent that disclosure is necessary to prosecute the violation or to continue the investigation

(2) A head, in determining whether a disclosure of personal information constitutes an unjustified invasion of personal privacy, shall consider all the relevant circumstances, including whether,

---

<sup>3</sup> Order PO-2560.

(a) the disclosure is desirable for the purpose of subjecting the activities of the institution to public scrutiny

(b) access to the personal information may promote public health and safety

(d) the personal information is relevant to a fair determination of rights affecting the person who made the request

(h) the personal information has been supplied by the individual to whom the information relates in confidence

(i) the disclosure may unfairly damage the reputation of any person referred to in the record

[16] In determining whether the disclosure of the affected party's information would be an unjustified invasion of personal privacy under section 38(b), therefore, I will consider and weigh the relevant factors and presumptions in sections 14(2) and (3) and balance the interests of the parties.<sup>4</sup>

### ***Representations***

#### *Police representations*

[17] The police submit that the report was created as part of a police investigation into a matter reported by the appellant, engaging the section 14(3)(b) presumption. They state that the withheld information relates to the identity of an individual suspected of a cybercrime involving a theft of Bitcoin and fraud, which was supplied by a third-party agency. They explain that law enforcement institutions have a unique authorization under the *Act* to collect personal information, and they view the spirit and content of the *Act* as placing a greater responsibility to safeguard the privacy of individuals when personal information is being collected. The police also reference Order M-655, where the adjudicator held that a finding of a section 14(3) presumption cannot be rebutted by the application of section 14(2) factors.

[18] Referencing the section 14(2)(h) factor, the police submit that police investigations are done with an implied element of trust that the law enforcement agency will act responsibly in the manner in which it deals with recorded personal information. They state that all records that could be released to the appellant were released. They submit that information that police collect from third parties is supplied with an expectation of a certain degree of confidentiality.

[19] The police acknowledge that the disclosure of the information may be relevant to the fair determination of the appellant's rights. However, referencing IPC Orders 12 and

---

<sup>4</sup> Order MO-2954.

P-224, they state that even if the information is relevant, the benefits of disclosure must be balanced with the protection of the privacy rights of individuals. They also refer to Order MO-1224, where the adjudicator distinguished access rights under the *Act* from disclosure in a criminal context. With respect to the section 14(2)(i) factor, the police state that it is not certain if the individual in the report is actually the perpetrator of the crime the appellant contacted the police about, and as such the release of the information may unfairly damage the reputation of an innocent party.

*Appellant representations*

[20] The appellant, through his representative, submits that disclosure of the information in the report would not be an unjustified invasion of personal privacy, and further submits that even if it were unjustified, the exemption is discretionary. Referencing section 14(3)(b), the appellant submits that even if the information was compiled as part of an investigation into a possible violation of law, the presumption does not apply to the extent that disclosure is necessary to prosecute the violation or continue the investigation. He submits that the information in the report would be used to prosecute the violation or continue the investigation into the individual's actions, and therefore the section 14(3)(b) presumption is not applicable to the appeal.

[21] The appellant submits that the information at issue is desirable for subjecting the group of scammers that the individual is a part of to public scrutiny, engaging the section 14(2)(a) factor. He also says that part of "public safety" relates to individuals not losing their money, engaging the section 14(2)(b) factor. He submits that, even if the information is highly sensitive (referring to the section 14(2)(f) factor, which the police did not directly address), the information should be disclosed due to the impact on the appellant and the amount that was taken via fraud.

[22] He submits that the personal information is relevant to the fair determination of his rights. He states that the right in question exists in law because fraud is an offence in the *Criminal Code*, and the information relates to a legal proceeding that will be brought to recover the money that was lost. He states that the personal information is significant to the determination of the right in question, and that it is required to prepare for the proceeding. He says that both criminal and civil proceedings will occur.

[23] He submits that without the individual's name, he will be unable to finalize the "Know Your Customer" (KYC) information and pursue legal remedies to recover the money. He states that without further action there is a good chance that the person who stole the money will continue to commit fraud against other victims. He generally states that the public interest is served by the release of information as well, but did not provide further details about this.

*Police reply representations*

[24] In response to the appellant's representations, the police emphasized that the

information at issue relates to a possible suspect in a police report, and reiterated that the section 14(3)(b) presumption against disclosure applies. They explain that following the police investigation, it was determined that there was insufficient evidence for any criminal proceedings. They state that there has been no confirmation that any of the perpetrators or the named individual are “actual involved parties” who knowingly took part in the fraud, and it is not known if the individual is indeed the perpetrator.

[25] They state that the release of this information may unfairly damage the reputation of an innocent party, and it would therefore be irresponsible to release any personal information to the appellant. They state that they advised the appellant to contact the third-party company for more information about the personal information he is seeking. Furthermore, they submit that the information is available to the appellant through other avenues, such as a court order.

#### *Appellant sur-reply representations*

[26] The police’s reply representations were provided to the appellant for a response, specifically regarding alternative means of accessing the information and how the appellant would use the information at issue to recover the lost funds. In response, the appellant said that he had contacted a recovery company who said that the name of the individual would “speed up” the process of recovering the lost funds, and recovery would be more difficult without the name. He also stated that he had contacted the third-party company himself and they refused to give him the information. He further explained that if a detective has the wallet address and KYC information for a suspected criminal’s account the account can be frozen by a judge, but he did not explain why this means that he needs the information, rather than this being done by the police.

#### ***Analysis and finding***

[27] As stated above, at issue in this appeal is whether disclosure of the information of the individual would be an unjustified invasion of their personal privacy under section 38(b).

#### *Presumptions and factors*

##### 14(3)(b): Investigation into a possible violation of law

[28] Under section 14(3)(b), the disclosure of an individual’s personal information to another individual is presumed to be an unjustified invasion of personal privacy if the personal information:

... was compiled and is identifiable as part of an investigation into a possible violation of law, except to the extent that disclosure is necessary to prosecute the violation of law or to continue the investigation.

[29] Even if no criminal proceedings were commenced against an individual, as is the

case in this appeal, section 14(3)(b) may still apply. The presumption only requires that there be an investigation into a possible violation of the law.<sup>5</sup> Based on my review of the report, the information in it was compiled as part of a police investigation into allegations of fraud where the appellant was the victim, engaging the presumption against disclosure in section 14(3)(b).

[30] The appellant submits that disclosure of the information would be necessary to prosecute the violation or continue the investigation, and the presumption therefore does not apply. However, it has previously been found, such as in Order PO-2236, that an appellant's own investigation, which the appellant appears to be referring to, does not constitute the continuance of the investigation referred to in section 14(3)(b), and the investigation referred to in the section is the one in which the information at issue was compiled. As such, I find that the section 14(3)(b) presumption applies.

[31] The police, referencing Order M-655, submit that the section 14(3) presumption cannot be rebutted by the section 14(2) factors. While I agree that this is a correct interpretation of the order, issued in 1995, it has been found in numerous orders since that under section 38(b) section 14(3) presumptions are not determinative.<sup>6</sup> In the circumstances of this appeal, where the record at issue contains the individual's personal information and that of the appellant, this presumption is not determinative, but instead a rebuttable presumption that can be weighed against the other relevant factors in section 14(2) below.

#### 14(2)(a): Subjecting institutions to public scrutiny

[32] Here, the appellant states that disclosing the information would promote scrutiny of the group of scammers that he says the individual is a part of. Based on the information before me, it is not clear if the individual belongs to such a group. In any case, this section supports disclosure when disclosure would subject the activities of the government (as opposed to the views or actions of private individuals) to public scrutiny.<sup>7</sup> It is intended to promote transparency of government actions. As the information at issue only relates to the individual, rather than any government institution (for example, it has not been established that disclosure of the information would in any way subject the police to public scrutiny), I find that this factor does not apply to the appeal.

#### 14(2)(b): Promoting public health and safety

[33] This section supports disclosure where disclosure of the information would promote public health and safety. In Order MO-1664, the factor was found to be intended to address records that contain information about public health and safety issues, rather than personal information about a particular individual who the requester may view as being a risk to public safety. However, in Order MO-3370, it was given moderate weight

---

<sup>5</sup> Orders P-242 and MO-2235.

<sup>6</sup> See, for example, Orders MO-2954, MO-4358, MO-4453, MO-4500, and MO-4503.

<sup>7</sup> Order P-1134.



favouring disclosure when a requester sought access to the name and address of the owner of a dog that bit her.

[34] Here, I generally agree that, as the appellant submits, "health and safety" extends to not losing money via fraud. However, even adopting the reasoning in Order MO-3370, it has not been established that disclosing the name of the individual would promote public health and safety. Unlike in Order MO-3370, where the factor was only given moderate weight, it is not even known if the individual was actually responsible for what happened to the appellant: he is only a suspect and the police have found that they do not have enough information to proceed with criminal charges. As such, I find that the factor should be given minimal, if any, weight.

14(2)(d): Fair determination of rights

[35] Both the police and appellant addressed this factor. The IPC uses a four-part test to decide whether this factor applies. For it to apply, all four parts of the test must be met:

1. Is the right in question a right existing in the law, as opposed to a non-legal right based solely on moral or ethical grounds?
2. Is the right related to a legal proceeding that is ongoing or might be brought, as opposed to one that has already been completed?
3. Is the personal information significant to the determination of the right in question?
4. Is the personal information required in order to prepare for the proceeding or to ensure an impartial hearing?<sup>8</sup>

[36] The appellant submits that all four parts of the test are met. The police appear to generally agree with this, but state that this is outweighed by the presumption against disclosure and other factors, and that the appellant can obtain the information through other avenues.

[37] Based on the information before me, it is clear that the right in question exists in law: the appellant was the victim of fraud and, aside from issues with identifying and locating the perpetrator, there may be legal avenues that he could potentially use to recover that money. Additionally, any proceedings that would be brought have not concluded, satisfying the second part of the test. However, having considered the representations of the appellant, I am not satisfied that the third and fourth parts of the test have been met. Alternatively, if they have been met, I find that the context of the

---

<sup>8</sup> See Order PO-1764; see also Order P-312, upheld on judicial review in *Ontario (Minister of Government Services) v. Ontario (Information and Privacy Commissioner)* (February 11, 1994), Toronto Doc. 839329 (Ont. Div. Ct.).

situation means that the factor should be given minimal weight.

[38] In his reply representations, the appellant stated that he required the information to “speed up” recovery of the money, and that recovery would be more difficult without the information at issue. The information at issue consists of the name, sex, and date of birth of an individual that the police identified based on a report from a third-party company, which used the Bitcoin wallet address to obtain this information. Based on the information before me, it is not known if the individual, identified only by a wallet address (that is not part of the withheld information), actually had a role in the fraud, or even if it’s the name of a real person.

[39] I agree with the police’s representations that the information can be obtained through other means, such as a court order. Indeed, in the appellant’s sur-reply representations he references steps that a judge can take to help him recover his money. That said, it has been found in recent IPC orders, such as MO-4500 and MO-4503, that individuals seeking information in police reports are entitled to access the information in the most efficient manner possible. The section 14(2)(d) factor was found to apply in these orders, and the information at issue was ultimately ordered disclosed. The present appeal presents a similar situation. However, although in those appeals it was disputed if there was any civil or criminal liability, the identities of the involved parties were not disputed. For example, in MO-4503, even if it was not clear that the affected party was civilly liable for the pedestrian-motor vehicle collision underlying the request, it was not disputed that he was the driver of the car.

[40] Here, although it is not disputed that a crime was committed, it is not known if the individual whose name is withheld in the report actually had any role in it. As such, it is not established that any legal proceedings related to the incident underlying the request would be properly directed at the individual. Based on this, I find that the personal information at issue, which may not even relate to the person responsible for the crime, is less significant to the determination of the right in question. I do not find that the factor should be given no weight: as the appellant submits, it is possible that the information may speed up the process of recovering the money. However, I do find that it should be given less weight than in situations where the identity of the person responsible for the incident underlying the request (for example the driver of a vehicle in a collision, or here the person who actually received the appellant’s money) is known.

14(2)(h): Information supplied in confidence

[41] The police did not directly reference section 14(2)(h) as a factor weighing against disclosure, but they state that the information was supplied with an expectation of confidentiality throughout their representations. This factor applies if both the individual supplying the information and the recipient had an expectation that the information would be treated confidentially, and that expectation is reasonable in the circumstances. Thus, section 14(2)(h) requires an objective assessment of the reasonableness of any

confidentiality expectation.<sup>9</sup>

[42] It may be the case that, as the police submit, the third party that provided the information to the police did so with an expectation of confidentiality. However, as the wording of the section makes clear (“supplied by the individual to whom the information relates”) it has previously been found that in order for the section 14(2)(h) factor to apply, the personal information at issue must have been supplied by the person who the personal information relates to.<sup>10</sup> In this case, the police obtained the individual’s information from a third-party agency, and the individual was not contacted. Considering this, I find that the section 14(2)(h) factor does not apply.

14(2)(i): Unfairly damaging the reputation of the individual

[43] The police submit that it is not known if the named individual was actually involved in the fraud where the appellant lost his money, engaging the section 14(2)(i) factor. This section weighs against disclosure if disclosure of personal information might create damage or harm to an individual’s reputation that would be considered “unfair” to the individual.<sup>11</sup> The appellant did not provide specific representations on this factor, but generally states that the rights of the individual should not be prioritized over the rights of the appellant, the victim in the crime.

[44] On its face, disclosure of a police report stating that an individual is suspected of a crime would damage their reputation. At issue in this appeal is whether such damage would be unfair. In Order P-602, the adjudicator considered if the factor applied to the disclosure of a preliminary report where there was no indication that the person in the report had acted inappropriately, and found that the factor applied. Similarly, in Order 151, it was found that if there is sufficient reason to question the accuracy or reliability of the personal information at issue, disclosure of it would unfairly damage the reputation of the party.

[45] Here, I find that the police report is similar to the preliminary report in Order P-602. While it is not disputed that the individual is named in the report, what this means is disputed. The police determined that they did not have enough information to proceed with criminal charges. It may be the case, given the different standards of proof for criminal and civil proceedings, that there is a civil case to be made against the individual. However, in either case, as the police submit, it is not clear that the individual is actually the perpetrator of the fraud that the appellant suffered. As such, I find that disclosure of the information could unfairly damage the individual’s reputation, weighing against disclosure of the information.

---

<sup>9</sup> Order PO-1670.

<sup>10</sup> Order P-606.

<sup>11</sup> Order P-256.

### *Balancing the factors*

[46] I have considered and weighed the representations of the parties, the section 14(3)(b) presumption against disclosure, the factors discussed above, and the access and privacy rights of the appellant and the individual respectively. While I understand the appellant's desire to recover the significant amount of money that he lost in the fraud, I find that when considering the presumption and factors in their entirety, particularly the uncertainty that the individual is in fact the perpetrator, the lack of clarity on how the information would actually assist with the recovery of the funds, and the alternative access methods available to the appellant, disclosure of the information would be an unjustified invasion of personal privacy under section 38(b). Accordingly, I uphold the decision of the police, subject to my review of their exercise of discretion, below.

### ***Exercise of Discretion***

[47] The section 38(b) exemption is discretionary and permits an institution to disclose information, despite the fact that it could withhold it. Having found that the withheld information in the report is exempt from disclosure under section 38(b), I must next determine if the police properly exercised their discretion in withholding the information. An institution must exercise its discretion. On appeal, the IPC may determine whether the institution failed to do so. The IPC may find that an institution erred in exercising its discretion where, for example,

- it does so in bad faith or for an improper purpose;
- it takes into account irrelevant considerations; or
- it fails to take into account relevant considerations.

[48] In either case, the IPC may send the matter back to the institution for an exercise of discretion based on proper considerations.<sup>12</sup> The IPC may not, however, substitute its own discretion for that of the institution.<sup>13</sup>

[49] The police submit that they did not exercise their discretion in bad faith or for an improper purpose, that they considered all relevant considerations, and that they did not take irrelevant considerations into account.<sup>14</sup> The appellant did not provide specific representations on the polices' exercise of discretion, but generally submits that if the information is withheld under section 38(b), the exemption is discretionary and the information should be disclosed.

[50] I have reviewed the considerations relied upon by the police and I find that they

---

<sup>12</sup> Order MO-1573.

<sup>13</sup> Section 43(2) of the *Act*.

<sup>14</sup> In their representations, the police state that they "took into account all irrelevant considerations." This appears to be a typographical error and I have interpreted it as such.

properly exercised their discretion in response to the access request. Based on their overall representations, it is clear that they considered the purposes of the *Act* and sought to balance the appellant's interest in accessing the full records with the protection of the privacy of other individuals when making their access decision.

[51] I find that the police did not exercise their discretion to withhold the individual's personal information for any improper purpose or in bad faith, and that there is no evidence that they failed to take relevant factors into account or that they considered irrelevant factors. Accordingly, I uphold the police's exercise of discretion in denying access to the withheld information.

**ORDER:**

I uphold the decision of the police and dismiss the appeal.

Original Signed by: \_\_\_\_\_  
Chris Anzenberger  
Adjudicator

July 12, 2024 \_\_\_\_\_