Policy Name:	**THREATS AND EXTORTION**		
Policy #:	OP 4.47	**Last Updated:**	2022-06-08
Issued By:	INVESTIGATIVE SERVICES BUREAU	**Approved By:**	SURREY POLICE BOARD
		Review Frequency:	AS REQUIRED

RELATED POLICIES

OP 4.15 *Cyber and Technology Crimes*

OP 4.30.3 *Statements – Victims & Witnesses*

OP 4.30.3.1 *Statements – Adult Suspects*

OP 4.30.3.2 *Statements – Youth Suspects*

OP 4.34.1 *Active Threat Response*

OP 4.52.1 *Trauma-Informed Practices*

OP 5.1.2 *Digital Evidence Management*

OP 6.1.1 *Victim Services*

1. PURPOSE

1.1. To establish procedures for the investigation of threats and extortion.

2. SCOPE

2.1. This policy applies to all Employees.

3. POLICY

3.1. During their duties Members may receive a complaint involving an allegation of threats or extortion.

i. "Uttering threats" occurs when a person knowingly utters, conveys, or causes a person to receive a threat to cause death or bodily harm to a person, to burn, destroy, or damage real

or personal property, or to kill, poison or injure an animal or bird that is the property of any person (see *Criminal Code*, section 264.1);

ii. "Extortion" is the act of using threats, accusations, menaces or violence to induce a person to do something or to cause something to be done. Extortion is often done to cause the victim to pay money (see *Criminal Code*, section 346(1)); and

iii. "Publication of an intimate image without consent" is when a person knowingly publishes, distributes, transmits, sells, or makes available an intimate image of a person, knowing that the person in the image did not give consent or being reckless to whether they gave consent or not (see *Criminal Code*, section 162.1).

a. When a person makes threats to distribute an intimate image to cause the person depicted in the image to do something or cause something to be done, this is sometimes referred to as "sextortion" and is the offence of "extortion".

3.2. When a report of threats or extortion is received, Members must conduct an evidence-based risk assessment to determine the threat level for the victim and must create a safety plan based on those risks.

3.3. Threats and extortion incidents can be extremely distressing to the victim(s). Trauma-informed practices must be used throughout the investigation, and a Victim Services referral must be offered where applicable. See OP 6.1.1 *Victim Services*.

4. PROCEDURE

Operational Communications Centre

4.1. When a call is received by the Operational Communications Centre (OCC) the call taker will obtain the following details:

i. caller and/or victim details;
ii. the nature of the extortion;
iii. what threats or demands have been made;
iv. any known suspect details (name, address, phone number, email address, screen username);
v. if any money has been exchanged and how much, what currency (cash, bitcoin, gift cards) and method (cash payment, money transfer); and
vi. how long has the situation been going on.

4.2. The call taker will tell the caller to retain all information including electronic communications received and that a Member will contact them.

4.3. The OCC call taker, with the assistance of an OCC Supervisor, will conduct an initial risk assessment to determine the priority in which the call should be dispatched to a Member for investigation.

i. Extortion which includes an active threat and/or kidnapping must be dealt with according to policy. Refer to OP 4.34.1 *Active Threat Response* and/or OP 4.34.7 *Hostage Taking and Kidnapping*.

Member

4.4. The investigating Member will:

i. using trauma-informed practices, obtain an audio or audio/video recorded statement from the victim and/or complainant to gather information about the circumstances and nature of the threat or extortion;
ii. obtain statements from witnesses, if any (see OP 4.30.3 *Statements – Victims & Witnesses*);
iii. open a PRIME-BC General Occurrence (GO) report and detail the initial investigation;
iv. depending on the nature, circumstances, and seriousness of the offence(s), consider discussing the file with Members from the appropriate Investigative Services Bureau unit;
v. if the suspect is known, obtain suspect details. If the suspect is not known, obtain as much information as can be provided by the victim and document the suspect as "unknown" in the GO;
vi. if available, obtain documentation, emails, electronic messages, chats, videos, etc., which provide evidence of the offence(s). Consider whether judicial authorization is required to obtain digital evidence from the victim's phone, computer, etc. (see *Regina v. Marakah,* 2017 SCC 59). Consider involving the Economic and Cybercrime Team if appropriate (see OP 4.15 *Cyber and Technology Crimes* and OP 5.1.2 *Digital Evidence Management);*
vii. ensure a safety plan has been discussed with the victim and that Victim Services has been offered (see OP 6.1.1 *Victim Services*);
viii. if an exchange of money has occurred, consider consulting an Economic and Cybercrime Team investigator for guidance and consider using a Production Order to obtain relevant financial records;
ix. if the identity of the suspect is known and if sufficient evidence exists, consider arresting the suspect. If appropriate, release them on the conditions (e.g., no contact) to enhance the safety of the victim or request Crown Counsel hold for court. **Note:** Extortion is a strictly indictable offence. Consider liaising with Crown Counsel for charge approval prior to arresting suspect;)
x. attempt to obtain a statement from the suspect. See OP 4.30.3.1 *Statements – Adult Suspects*; OP 4.30.3.2 *Statements – Youth Suspects*;
xi. if grounds exist, forward a Report to Crown Counsel and recommend the appropriate charges; and
xii. If no other investigative avenues can be pursued, conclude the file. If the file is to be concluded, explain the rationale to the victim and ensure they have the necessary support.

Supervisor

4.5. If the file is maintained in the Community Policing Bureau, the assigned Member's Frontline Supervisor will periodically review the investigation and ensure that the investigator is conducting a thorough investigation in accordance with this policy. If necessary, the Supervisor must assist by

liaising with Supervisors from other investigative units who may be able to provide guidance to further the investigation.

4.6. If a unit or team from the Investigative Services Bureau takes conduct of the investigation, the unit or team Supervisor must ensure that the investigation is maintained and reviewed as required by the unit's or team's Investigative Business Rules.

APPENDIX A: DEFINITIONS

"Employee" means a sworn Police Officer or a civilian Employee appointed by the Surrey Police Board.

"GO" means a General Occurrence report in PRIME-BC.

"Member" means a Sworn Officer appointed by the Surrey Police Board.

"OCC" means the Operational Communications Centre.

"PRIME-BC" means the Police Records Information Management Environment, British Columbia's police records management system.

"Supervisor" means a Sergeant, Staff Sergeant, Sergeant, Inspector, Superintendent, Deputy Chief Constable, Chief Constable, and any other person acting in a Supervisory capacity who is accountable for a particular area or shift on behalf of SPS.

APPENDIX B: REFERENCES

Criminal Code, R.S.C. 1985, c. C-46