Business case for Financial Crime Unit

APPENDIX D

Examples of files affected by federal re-engineering

RCMP Detachment Economic Crime Units (ECU) were contacted for this report. They were asked to submit some examples of files that were not fully investigated (or investigated at all) due to resource issues, being too large or complex, multi-jurisdictional, etc. Responses were received from Richmond, Surrey, Kelowna and UBC detachments. Some of the examples are as follows:

- **"Advance fee" fraud** (FSOC 2014-497): A Richmond, BC resident had been committing an "advance fee" fraud amounting to $2.5 million over a ten year period. West Kelowna detachment hired a reserve constable with a background in commercial crime. The investigation was started but the file was shut down as more were resources were required which could not be provided. In 2016 the FBI in Alabama indicted the same suspect for a similar fraud of $3.8 million.
- **Theft and Use of Credit Cards** (Kelowna 2015-53463): An organized crime group was identified that was involved in the stealing credit cards from vehicles across the Lower Mainland and Okanagan and making numerous purchases with those cards. A large team of investigators across the province was required for surveillance and to collect further evidence. As there were no resources to investigate, the targets were not investigated and continued to commit numerous offences across the province.
- **Data Breach at Interior Health** (Kelowna File 2014-54234 and seven associated PRIME files): A suspect obtained employee information which was used to obtain credit cards in employees' names and went on a shopping spree in Alberta. The victims originated from the Okanagan and the Kootenays. Numerous files were opened up across the province since this was a multi-jurisdictional offence.

However, no proper investigation was conducted as it was too large for one detachment to manage.

- **Flight Centre** (Kelowna file 2014-44028): Twenty-five Flight Centre locations across Canada, including numerous ones in BC, were defrauded of $63,000. The investigation from Kelowna identified viable leads to be followed up in the Lower Mainland, however no unit was willing to continue the investigation and the file was eventually concluded.
- **Government of Canada Cheques** (Kelowna file 2014-62522): Government cheques were compromised in eastern Canada and counterfeit cheques were cashed at banks all across BC. There were no resources to investigate and to link the occurrences together.
- **Go Max Solutions** *(data storage company for mortgage companies within Okanagan)* (Kelowna File 2016-49019): A suspect hacked into the company's database which contained personal information of approximately 400,000 clients. The investigation revealed suspects may have hacked the system from the United States. There were no resources within the Kelowna ECU with the capacity to investigate the hacking and link together any resulting frauds.
- **Law Firm – Theft (**Richmond File 2016-10431): A subject reported that her law firm accountant took $7 million from the firm's trust account. The money was obtained from the trust account by way of pre-signed cheques that were kept on hand at the law firm. Richmond ECU advised that there were issues as it involved records located at a law office which involved solicitor-client privilege. Regional Crown counsel expressed surprise that these investigations are now only conducted by the police forces of jurisdiction.
- **Investment Scheme** (Richmond File 2015-37775): A business owner lost $1.7 million in a scheme that involved a logging and power generation operation in Chile. Due to the complexity of the file, it was successfully passed over to the Criminal Investigation Unit of the BC Securities Commission. According to the Richmond ECU, in previous years such a file would have been referred to the Commercial Crime Section.

- **GPUN Broadway Investment Inc. – Fraud** (Richmond File 2016-3630): Seventeen investors contributed a total of $6 million for a real estate venture involving two companies. Based on the contracts and the complexity of this investigation, this file would also have not have been investigated by Richmond ECU prior to the folding of the Commercial Crime Section.
- **Crown Counsel – Fraud** (Surrey File 2012-97775): This was a fraud file involving a now former Crown counsel in Surrey. The file was referred to FSOC, however it was determined to be of too low a dollar value to meet the threshold of a serious or organized crime file. At issue was that a Crown prosecutor in Surrey, which members in Surrey regularly deal with, was being investigated by Surrey ECU.
- **CentrePoint - Investment Fraud** (Surrey File 2014-73062): A large securities fraud that involved multiple investors, shell companies, SEC filings, MLATs, and one suspect in the US and one in New Zealand. Surrey ECU passed it off to the BC Securities Commission since they could not handle it.
- **Mail Theft/Fraud Ring** (Surrey File 2015-48138): A large fraud in which Surrey ECU was able to lay a couple of charges, primarily based on possession of materials. Surrey ECU did not have the resources to investigate the tens of thousands of dollars of fraud through the RBC corporate rewards points system, a mail theft ring, organized crime ties, or a conspiracy component.
- **Interior Health/ Identity Fraud** (Surrey File 2015-86007): Surrey ECU received a report that a subject had somehow obtained a database of Interior Health employees' information. Surrey ECU seized a USB containing the spreadsheet but were unable devote the resources to determine how Interior Health was compromised, who obtained the information and where or how that information was used.
- **CRA Tax Payment Fraud** (Surrey File 2015-179097): Surrey Detachment received numerous reports of a CRA tax fraud scam. Surrey ECU required this to be a major project in order to tackle the issue, and it was determined that it was beyond Surrey ECU's capabilities or mandate.

- **International Lottery Fraud** (Surrey File 2016-32746/135938): Surrey ECU is in the process of referring the file to FSOC as this relates to international money laundering, extensive coordination with international law enforcement partners, and evidence will likely lead to organized crime in the Lower Mainland. If this file is not investigated by FSOC, Surrey ECU will not have the resources to investigate.
- **Employee Fraud (UBC 2014-559):** UBC to the University Detachment that the now-fired Assistant Dean of Dentistry had allegedly defrauded them of $4.3 million over 11 years. Vancouver Police commenced a parallel investigation involving the same suspect allegedly defrauding Vancouver General Hospital. Shortly after federal re-engineering, both units requested Federal Serious and Organized Crime to take the lead on their investigations but the request was denied, as FSOC was not in a position to take on the investigation. Vancouver Police concluded its file to the University Detachment, which subsequently concluded its file due the magnitude of the investigation.
- **Global Mail Redirection (Coquitlam / FSOC 2014-7083, and ten associated PRIME files):** Multiple orders for counterfeit identity documents were intercepted by the Canadian Border Services Agency from the UK, USA and Australia. They were destined to a person who had a record for identity theft. There was interest by Homeland Security Investigations, Canada Border Services Agency and Canada Post, but lack of resources in E Division Federal Serious and Organized Crime did not permit an investigation to be done.
- **First Nations (VPD 2016-94549):** A large file involving defalcation by a controller employed by an employment society operated by First Nations groups from around the Lower Mainland and funded by the Federal Government. The file came to the Vancouver Police Department's attention as the main office had been located in Vancouver. VPD declined to investigate as numerous jurisdictions outside of Vancouver were involved, the only connection to Vancouver was the single operating office and VPD did not have the resources to conduct the investigation.

- **Identity Theft / Loan Fraud (Kelowna File 2016-39751):** This crime involved a very sophisticated organization of several individuals in British Columbia and Alberta. The suspects registered fake Trade Names with Service Alberta and subsequently opened bank accounts using the fake Trade Names. A fake business was created based out of Grand Prairie, Alberta that sold heavy equipment. A leasing company in Kelowna, BC was used to facilitate loans through a Credit Union that was the ultimate victim that lost $510,000. The majority of the money was used to purchase gold in BC and Alberta. This would be more suitable for a provincial unit to take on as it has the elements of Organized Crime and is multijurisdictional.
- **Theft / Use of Credit Cards (Kelowna File 2017-7278):** This investigation involved a travelling organized group that stole credit cards from vehicles, would change the PIN, and then commit fraudulent transactions. This group had been the subject of numerous files throughout many jurisdictions in BC. A provincial unit would have the resources to dedicate to following and tracking this group through the jurisdictions in order to gather enough evidence for charges indicative of the level of crime this group is committing.
- **Fraud / Theft / Breach of Trust (Midway File 2013-905):** In April 2013, the Rock Creek & Boundary Fair Association (the Association) reported a fraud involving a treasurer with a value over $200,000. Due to the small size of the detachment, the file was bounced around to multiple investigators. Three years later, an RTCC was completed and sent to the Commercial Crime Section in Vancouver. The RTCC was returned to the detachment with a long list of “to do’s” which continue to be worked on today. On November 15, 2017, the Association wrote a letter to the Deputy Commissioner of “E” Division expressing their dissatisfaction with the delays. This example further outlines the need for a provincial unit to either take over the file or provide the assistance and guidance necessary to assist detachments that don’t have the resources or the expertise to work on large and/or complex fraud files.