

SNOHOMISH COUNTY PROSECUTOR'S OFFICE INVESTIGATIVE CHECKLIST

UNLAWFUL FACTORING OF CREDIT CARD OR PAYMENT CARD TRANSACTION

RCW 9A.56.290

ELEMENTS

For the Class C Felony crime:

- 1a. The suspect used a scanning device to access, read, obtain, memorize, and store, temporarily or permanently, information encoded on a payment card; AND
- 1b. The suspect did not have the permission of the authorized user of such card; OR the suspect intended to defraud the authorized user, another person, or a financial institution.

OR

- 2a. The suspect used a re-encoder to place information encoded on a payment card onto a different payment card; AND
- 2b. The suspect did not have the permission of the authorized user of the card from which the information was encoded; OR the suspect intended to defraud the authorized user, another person, or a financial institution.

OR

- 3a. The suspect presented to or deposited with, or caused another to present to or deposit with a financial institution, for payment, a credit card or payment card transaction record; AND
- 3b. The credit card or payment card transaction record was not the result of a credit card or payment card transaction between the cardholder and the defendant.

OR

- 4a. The suspect employed, solicited, and otherwise caused a merchant* or an employee, representative, or agent of a merchant to present to or deposit with a financial institution, for payment, a credit card or payment card transaction record; AND
- 4b. The credit card or payment card transaction record was not the result of a credit card or payment card transaction between the cardholder and the merchant.

OR

- 5. The suspect employed, solicited, or otherwise caused another to become a merchant* for the purpose of any of the four alternatives above.

AND, for the Class B Felony crime:

- 6. The suspect previously was convicted of Unlawful Factoring of Credit Card or Payment Card Transaction.

*Merchant means an owner or operator of any retail mercantile establishment or any agent,

employee, lessee, consignee, officer, director, franchisee, or independent contractor of such owner or operator. "Merchant" also means a person who receives from an authorized user, a payment card or information from a payment card, or what the person believes to be a payment card or information from a payment card, as the instrument for obtaining, purchasing, or receiving goods, services, money, or anything else of value from the person.

SPECIFIC REQUIREMENTS

- [] 1. If illegal scanning device or illegal re-encoder seized, identify expert witness who can examine the device and the information stored in it (pursuant to a search warrant) and testify about how the device functions and what information is stored in it.
- [] 2. If seized, a copy, front and back, of all *stolen* credit cards and payment cards and of *fraudulent* credit cards and payment cards. If seized, a copy of all *stolen* credit card and payment card transaction records and of *fraudulent* credit card and payment card transaction records.
- [] 3. When fraud scheme evidence is seized from a location other than a legitimate business and where multiple people have access to it, determine who had access to the items by, for example, seizing papers of occupancy/ownership for the building/vehicle where found; obtaining witness statements; latent prints; etc. If evidence is found in a bedroom, seize sample clothing items in bedroom to establish sex/size of bedroom occupants.
- [] 4. If suspect used a legitimate scanning device to obtain information from a credit card or payment card with fraudulent intent, obtain evidence to establish suspect's access to the scanning device, such as a statement from the suspect's employer regarding the suspect's work hours, duties, access to credit card scanner, etc. Can all others who had access to the device be ruled out? How?
- [] 5. If fraudulent credit card or payment card transaction records were presented or deposited to a bank, statement from bank employee regarding the details of the transaction and whether the bank employee can identify the person presenting or depositing.
- [] 6. Victim account holder's statement should specifically identify the transactions that were legitimate and the ones that were fraudulent.
- [] 7. Statement from custodian of records for the credit card company or issuer of payment card documenting the unauthorized use of the credit card or payment card.
- [] 8. Copy of police reports regarding the theft of any credit cards, payment cards, credit card transaction records, payment card transaction records, mail, identification cards, etc. found with the fraudulent credit card and payment card transaction records.
- [] 9. Obtain from suspect, if possible, detailed information regarding the fraudulent scheme and who was involved. Provable lies are as worthy as admissions.
- [] 10. If computer equipment seized, search computer (pursuant to a search warrant) for evidence of fraudulent scheme.