THREAT HUNTER RESEARCH

The Auto Loan Fraud Industry Chain

A study of the intermediaries, forged materials and vehicle-disposal practices that connect the auto-loan fraud chain.

Original publication: 2024-11-29
Research team: Threat Hunter Research Team
Source report: 19 pages

Original report text

This text version is reconstructed based on the 19-page original PDF, retaining the report narrative, chapters and research scope; the cover, duplicate table of contents and purely decorative pages are not repeated. Localized figures are placed in context throughout this web edition, with the original PDF retained for reference.

Preface

In recent years, the auto finance market has continued to expand, and auto loan fraud has become increasingly rampant. Threat Hunter's investigation found that illegal threat actors, under the banner of "financing a car," "purchasing a car with 0 down payment," and "cash out a car," recruit some people who are unable to obtain financing through normal loans but have financial needs, such as households with white credit, poor households, black households, etc., and carry out contract fraud and loan fraud by "fake car purchases, real cash out" through identity packaging. Among these people who "finance cars", there are many "professional debtors".

(People's Daily News: Ningxia Helan County Public Security Bureau busted a car loan fraud gang)

Based on Threat Hunter's in-depth research on the auto loan fraud industry chain, this article objectively presents customer recruitment techniques, packaging techniques, vehicle disposal, and fraud intensity in different regions in auto loan fraud, providing reference for loan-risk management strategies of banks and other financial institutions.

Secondary sale).

Auto loan fraud risk overview

1. Overview of Auto Loan Fraud Risks

1.1 Overview of Auto Loan Fraud

Threat Hunter learned that threat actors recruit some "customers" who cannot obtain financing through normal loans but have financial needs, provide them with a series of packaging and professional guidance, and help them buy cars through loans from financial institutions. After the customers pick up the car license plate, they mortgage or sell the vehicle through third-party channels to cash in (such cars are often quasi-new cars and "0-kilometer used cars"). "By operating a car in three days, one person can make multiple car loans, and even apply for multiple loans for the same car." In the end, such cars are resold to other places through layers of layers, sold domestically or laundered and exported.

After completing the loan, the customer can choose to "want the money but not the car" or "want the car but also the money". After the car is financed and cashed out, the amount the customer receives is 40% to 60% of the total value of the vehicle, or even less, and the remaining amount is divided up by threat actors. In order to delay the scam being discovered, threat actors usually leave part of the money to help customers repay or ask customers to repay normally for 3 to 6 months. After the due date, they refuse to repay due to other force majeure factors or emergencies, thereby paralyzing financial institutions and evading public security agencies.

The following is the operation process of car financing risks in recruitment, packaging, application, advance payment, car pickup, license plate, vehicle disposal and other links:

1.2 Regional distribution of auto loan fraud popularity

Overview of auto loan fraud

Source: Threat Hunter original report, page 5

Threat Hunter's analysis of auto "car financing" fraud intelligence in the third quarter of 2024 found that among provinces (including municipalities), Guangdong, Hunan, and Guangxi have higher levels of auto loan fraud. Among cities (including municipalities), Changsha, Guilin, and Chongqing have the highest fraud rates, and Changsha's car loan fraud rate is much higher than other cities.

The three provinces with the highest prevalence of car loan fraud in the third quarter of 2024: Guangdong, Hunan, and Guangxi The three cities with the highest prevalence of car loan fraud in the third quarter of 2024: Changsha, Guilin, and Chongqing

Analysis of car loan fraud operation methods

2. Analysis of car loan fraud operating techniques

2.1 Recruiting target customers

2.1.1 Recruitment direction

Regional heat of auto loan fraud (Chart 1)

Source: Threat Hunter original report, page 6

Regional heat of auto loan fraud (Chart 2)

Source: Threat Hunter original report, page 6

The There are two main recruitment directions for actors. One is regular cash-out recruitment. The target customers are customers who have financial needs but cannot obtain loans through mortgages and credit normally. Such customers hope to meet their personal emergency capital needs by cashing out car loans, have a subjective willingness to repay, and do not intend to defraud loans. The other is "professional debt" cash-out recruitment, through multiple types of "housing/credit/business/car" loan combinations, such as cashing out car loans, and operating personal credit, housing loans, and corporate loan-related loans before and after the same period. This kind of loan is a loan where the customer has no willingness to repay and is intended to defraud the loan.

2.1.2 Recruitment techniques

threat actors and black intermediaries generally use social software and small video platforms to collect credit information across the country for "white households", "small flower households" or customers who cannot mortgage credit but have financial needs. They are about 25-50 years old. They are required to be able to speak and write, be able to handle the lender's loan approval, and be able to communicate and implement the special requirements of threat actors.

threat actors gather qualified customers who are willing to finance cars or take on debt into the car loan operation area and live there for a short period of time in order to cooperate with the various operations of threat actors. Such customers are usually arranged to stay in hotels, simple residential houses or simple hotels. threat actors implement a "three guarantees" policy of including food, accommodation and travel expenses.

If the customer is in debt, after the car loan is processed, they will be transferred to other cities according to the requirements of threat actors to continue operating housing loans, credit or business loans. In addition, some car salespeople will also publish some sales advertisements, cooperate with loan intermediaries and threat actors to acquire customers, and even assist customers in financing cars by default.

The following is a recruitment advertisement for threat actors:

After the target customer is determined, the customer does not even need to go to the car dealer to look at the car and choose a car. The threat actors directly select the loan model for the customer. The customer only needs to cooperate in the follow-up. For example, the customer can conduct pre-approval in another place. After passing the pre-approval, go to the car dealer city to operate the subsequent loan process.

Before threat actors apply for loans to customers, they will make a series of preparations, such as customer identity packaging, flow packaging, etc., to ensure the smooth disbursement of car loans. It usually takes 1 to 3 days to complete a car loan from applying for a loan to settling in and picking up the car.

2.2 Analysis of packaging techniques

Whether it is a regular car loan cash-out or a debt-taking cash-out, threat actors will package different situations according to the basic situation of the customer before operating the loan. The packaging technique is mainly reflected in the packaging of the customer's identity, such as advancing funds to buy a house and packaging them as a real estate householder, through corporate transfers as a business owner, paying social security provident funds to the customer and packaging them as a salaryman, etc. It is also reflected in packaging false income flow for the customer, and also in maintaining the customer's credit report, etc.

2.2.1 Identity packaging techniques

Identity packaging is divided into false packaging and real packaging. False packaging refers to packaging through false information, such as filling in a false work unit, false social security provident fund, personal tax app, etc. to package work identity; real packaging refers to packaging through "real" actions, such as real house purchase, real transfer of enterprise, real payment of social security provident fund, regular transfer to the customer's salary card as salary, etc.

In the process of real identity packaging, threat actors need to advance a large amount of capital or make an upfront loan (credit/mortgage) to the customer as the initial packaging cost. This operation method requires a large capital cost, but it can also loan a higher amount, which is a huge profit driver, forming a high-cost and high-yield "housing, credit, enterprise, car" large-amount comprehensive debt business. threat actors package real estate and companies as credit enhancement conditions for customers, and are often able to apply for high-priced car loans, and even get multiple loans for one car or one person.

2.2.2 Income flow packaging techniques

For customers with good overall qualifications, such as credit conditions and big data qualifications, which basically meet the requirements of financial institutions for car loans, but if the customer does not have a social security provident fund or a stable income, which will affect the approval rate and approval amount of the car loan, the loan intermediary can package the customer's income flow at a low cost.

According to the different verification methods of car loan customers' income by different financial institutions, intermediaries also have different packaging methods, such as social security provident fund, personal tax, bank statement, WeChat statement, Alipay statement, etc., which can reflect the customer's income. The intermediary will join forces with threat actors who specialize in producing false statements to produce fake paper versions, electronic versions, and bank apps at a cost ranging from hundreds to thousands of yuan according to the verification requirements of the lending financial institution. He used fake transaction materials to bypass fraud controls and successfully applied for a car loan business.

2.2.3 Maintenance of credit reporting packaging techniques

threat actors aims at mortgage-free customers who have a "Motor Vehicle Registration Certificate" (hereinafter referred to as the "big book"), which can be transferred and cashed out normally, and the cashing profit is large.

At present, some threat actors will call target customers to cash out their car loans in areas with exemption policies or loose mortgage policies, such as Xinjiang, Shaanxi, Ningxia, Gansu, Qinghai and other places. If the customer's qualifications are not enough to apply for a credit-free car loan, threat actors will package or maintain the customer's credit report based on the customer's situation. The maintenance period is 3-6 months, and artificial adjustments will be made based on the customer's credit report inquiry, such as maintaining the customer's credit report inquiry to no more than 3 inquiries in the past 6 months, packaging the customer's workplace, etc. After the customer's qualifications meet the car loan requirements, the customer will be able to cash out the car loan.

2.3 Vehicle Disposal

Car loan products of different financial institutions have different handling methods for subsequent vehicle control, which are mainly divided into two situations: one is mortgage-free, and the other requires mortgage.

Mortgage-free: means that after a customer buys a car through a loan, he or she does not need to mortgage the vehicle to the lending financial institution, and the capital is directly kept by the customer; mortgage means that after the customer purchases a car through a loan, the lending financial institution requires the customer to mortgage the vehicle to the lending financial institution in order to control post-loan risks, and the capital is handed over to the lending financial institution for safekeeping until the customer settles the payment and the financial institution returns the capital to the customer.

According to whether the vehicle is truly mortgaged to the lending financial institution, it is divided into true exemption and false exemption:

True exemption: refers to the mortgage-free car loan products of some financial institutions or the mortgage-free loan method implemented by some financial institutions for customers with particularly good credit conditions and high-quality units.

Fake credit exemption: Also called forced credit exemption, it refers to a vehicle purchased through a mortgage loan. According to the requirements of the loan process, the purchased car should be mortgaged to the lending financial institution after the car is registered. However, threat actors cooperate with the customer to sell the vehicle to a third party before the mortgage period

of the financial institution and transfer it to the third party. The car cannot be mortgaged to the financial institution. This is not a true mortgage-free car loan.

According to the different subsequent management methods of vehicles by financial institutions, the methods used by threat actors to cash out vehicles after financing are also different. The resale flow of vehicles is domestic sales or laundering for export or dismantling and selling parts. Cash-out methods mainly include the following two aspects:

First, the vehicle that has been mortgaged to a financial institution is mortgaged again to a stolen auto trading company or a third party for cash or dismantled parts for sale. Since this kind of car cannot be transferred, it can only be used as a black car. The cost of cashing out is high, and the amount received by the customer is 20%-30% of the value of the vehicle, or even less. In addition, due to the low selling prices and low profits of such black cars, some threat actors directly work with third parties to dismantle the vehicles and sell related parts to auto repair companies or 4S stores.

Second, vehicles that have not been mortgaged to financial institutions (cars that are free of charge or that have not yet reached the mortgage period) can be directly sold to a stolen auto trading company or a third party for cash as long as the customer has a large amount of capital. Such vehicles have complete procedures and can be transferred normally, and the amount received by the customer is 60%-80% of the value of the vehicle. This cash-out method is highly profitable and has become a mainstream cash-out method.

Threat Hunter Financial Loan Anti-Fraud Services

3. Threat Hunter financial loan anti-fraud service

Whether the “car financing” behavior is a regular cash-out or a professional debt-taking cash-out, threat actors will basically package customers and beautify their qualifications before applying for loans, which poses the risk of gang attacks. This type of customer is not the target customer group of financial institutions, and their repayment ability is extremely low, and they may even have no willingness to repay. The risk of loan overdue is extremely high, which will cause immeasurable losses to the lending financial institutions.

Threat Hunter focuses on the field of financial cybercriminal groups attack and defense. By covering various intelligence channel sources, it actively obtains a large amount of credit threat actors/black intermediary data, and automatically extracts the characteristics of the target fraud group based on the fraud characteristic analysis model. At the same time, combined with the in-depth analysis of experts from the Digital Risk Response Center (DRRC), it builds a credit anti-fraud closed loop for financial institutions from the latest fraud risk perception, business/fraud-control strategy guidance, to the positioning of malicious loan groups.

3.1 Timely sense and warn against the latest credit fraud risks

Threat Hunter comprehensively monitors the credit business and various business links of financial institutions. Credit fraud intelligence experts actively operate on credit risk clues across the entire network to promptly perceive the latest fraud risks of threat actors/intermediaries, including fraud techniques, fraud scenarios, etc., such as fraud risk monitoring involving real estate credit/enterprise/car/cash/decoration/consumer loans/beauty loans and other loan businesses.

3.2 Provide business fraud-control strategies based on group portraits

Threat Hunter's credit fraud intelligence team goes deep into different credit fraud scenarios, analyzing and reproducing the entire fraud process from an attacker's perspective, including providing financial institutions with analysis of designated fraud links, such as customer acquisition techniques, packaging methods, business operation processes, etc., and establishing the business behavior characteristics of fraud groups for financial institutions through different scenario analysis reports, providing interpretable basis for fraud-control strategies.

3.3 Locate malicious fraud groups based on valid tags and other data

Based on continuous monitoring and correlation analysis of the credit fraud industry chain, Threat Hunter can obtain a large number of group characteristic information (such as identity information, bank card information, etc.) of effective fraud groups, and can help financial institutions conduct correlation analysis based on malicious feature tags based on security detection measures such as big data models to accurately locate fraud groups.

Explanations of related terms and definitions of "black words"

4. Explanations of related terms and definitions of “slang”

Baihu: usually refers to those with little or no credit history. Individuals in this situation have no past lending history, making it difficult for banks or lending institutions to accurately assess their credit risk. It belongs to the material category in the cybercrime ecosystem chain and is often sold on TG, Twitter, and potato. Fraudsters may use this "white account" identity to commit credit fraud, such as applying for loans by fictitious credit information or forged documents. This strategy allows them to obtain credit without banks and financial institutions knowing their credit history. These people involved in debt-bearing are also called "white debtors" or "professional debtors."

Huahu: Refers to people who frequently apply for credit cards or loans. This behavior may be viewed as a higher risk characteristic by financial institutions, as frequent applications for credit cards or loans may indicate that the individual has urgent financial needs or that there are issues with his or her credit management.

"Flower households" often show a large number of credit inquiry records on their personal credit reports, which may have a negative impact on their future credit applications. "Huahu" may also be used by threat actors for credit fraud, such as in "debt restructuring", where threat actors help

users pay off their debts through early advances and then burden them with higher amounts of loans.

Xiaohua/Small Flower Household: It is a type of Huahu. Compared with the Big Huahu, the Big Huahu refers to the customers who have a lot of credit inquiries, a large number of loans, and poor credit, while the Xiaohuahu refers to the customers who have a relatively small number of credit inquiries, a relatively small number of loans, and a relatively average credit.

Black account: usually refers to individuals who have bad credit records and have been blacklisted by banks. These people may be blacklisted by financial institutions due to loan arrears, defaults or other bad credit behaviors, which means that it is difficult for them to obtain loans or credit cards through formal channels. Black accounts are sometimes used by cybercrime ecosystem operators for money laundering, that is, by transferring illegal gains through these accounts to disguise the illegal source of the funds. Cybercriminal groups may use the personal information of black accounts to try to conduct credential stuffing attacks in different financial institutions to see if this information can be used to successfully apply for loans or credit products.

Car Financing: Often refers to the act of obtaining a car loan or lease using false information or deceptive means. By "packaging" personal information, financial status, and employment status, threat actors bypass fraud controls and obtain car loans with unreal car purchase needs, and then dispose of the vehicles to cash out, which is called "car financing and cash out." It also refers to a method of disguising transactions, that is, deceiving lending institutions through fictitious car sales transactions.

III. Financial loans against fraud services that Threat Hunter

Source: Threat Hunter original report, page 14

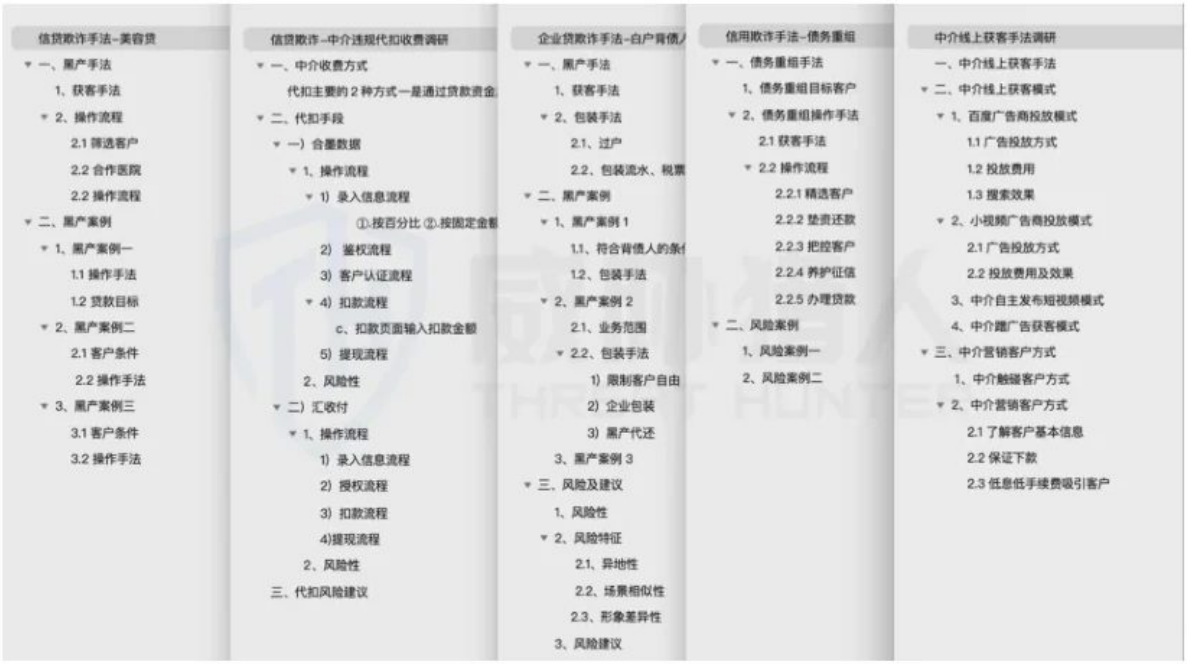
For example, if you apply for a loan or lease based on a fictitious car sales contract, no real car transaction actually occurs.

Big book: In car loan fraud, refers to the motor vehicle registration certificate, also known as the "green book".

True exemption: refers to the mortgage-free car loan products of some financial institutions or the mortgage-free loan method implemented by some financial institutions for customers with particularly good credit conditions and high-quality units.

Fake credit exemption: Also called forced credit exemption, it refers to a vehicle purchased through a mortgage loan. According to the requirements of the loan process, the purchased car should be mortgaged to the lending financial institution after the car is registered. However, threat actors cooperate with the customer to sell the vehicle to a third party before the mortgage period of the financial institution and transfer it to the third party. The car cannot be mortgaged to the financial institution. This is not a true mortgage-free car loan.

Point: refers to the fee extracted by cybercriminal groups. The point size is judged by the risk level. The higher the risk of the source's funds, the higher the point of threat actors.



The credit fraud landscape is organized according to fraud techniques, operating processes, cases and risk recommendations.

Source: Threat Hunter original report, page 15