THREAT HUNTER RESEARCH

Fabricated Bank Statements in Credit Fraud

An investigation into fabricated bank statements, document-authenticity risks and their implications across the credit lifecycle.

Original publication: 2024-09-12
Research team: Threat Hunter Research Team
Source report: 18 pages

Original report text

This text version is reconstructed based on the 18-page original PDF, retaining the report narrative, chapters and research scope; the cover, repeated 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

Bank statements record the details of capital transactions of enterprises and individuals, reflecting important information such as cash flow and operating performance of the entity. In our country, bank statements are an important document proving the creditworthiness of an entity and are widely used in public and private financing, equity investment and other businesses.

The real statement refers to the statement printed out through the bank counter. On the contrary, fake statements refer to fictitious statements made through threat actors, intermediaries and other channels.

In the credit scenario, some people are unable to apply for loans normally due to problems such as incompatible qualifications and lack of conditions, and can only achieve the purpose of borrowing and financing through "false data" such as false demand and false flow. Currently, banks or lending institutions cannot directly access personal and corporate flow information from other banks. Loan customers are required to provide relevant flow information independently and complete the corresponding loan review. This provides an opportunity for threat actors to provide customized and false personal and business flow information to help loan customers pass loan approval and obtain higher loan amounts.

The following is an incident involving a car loan fraud gang busted by Yinchuan police, which involved the fraud gang using fake jobs and fake income to apply for car loans to debtors:

At present, the fraud techniques of threat actors are constantly being updated and iterated, and they are becoming more real. The false flow may be used by threat actors for any loan product that needs to verify the income level to evaluate the repayment ability but has not verified or cannot verify the third-party official interface data.

Secondary sale).

Types of false turnover and malicious activity procedures

1. Types of false transactions and malicious activity-doing processes

The false flow mainly involves paper version flow, PDF flow, high and low configuration mobile phone app flow, and official bank app flow. The display method involves app versions such as banks and third-party payment platforms; the flow direction involves transaction flow data such as punch-in wages, collection codes, and corporate accounts. The following is some recruitment advertising information for threat actors discovered by the Threat Hunter intelligence research team:

The black financial intermediary determines the required type of transaction based on the customer's qualifications and corresponding target loan product needs, and specially customizes

the paper version or PDF version or the fake bank app version or the bank's official app version with the forged threat actors. And different types of fake sales have different prices and operating procedures.

1.1 Paper/PDF flow

Original report charts, processes and cases

Source: Threat Hunter original report, page 3

Paper/PDF fake statements refer to bank statements produced through forgery and presented in the form of paper or PDF electronic documents. The paper version and PDF version have the lowest cost of counterfeiting and the narrowest level of use. They are suitable for loan scenarios that only require customers to provide paper materials or PDF versions, or in scenarios where there is collusion between internal and external bank personnel. The production cost of this paper/PDF version is relatively low, with a price of around 200-300 yuan.

The financial intermediary puts forward the demand for the flow production results based on the customer's situation, such as the length of the flow cycle, account information, monthly income, balance and other requirements. The threat actors operate the flow transaction record sheet in the background based on a certain bank's official flow format, official seal and other information. After the flow sheet is completed, it is sent to the intermediary in PDF format. The intermediary then prints the paper version of the flow sheet or directly submits the PDF version of the flow sheet to apply for a loan.

Under normal circumstances, threat actors who create false reports only provide electronic or PDF versions, and do not provide data sources to intermediaries or customers, similar to the model where some photography agencies only provide photos and do not deliver negatives. Financial institutions can verify the authenticity of the flow by verifying the data on the app side. For example, if the customer provides an electronic version of the punch-in salary flow, the authenticity of the data can be verified by on-site verification of the customer's mobile banking app.

The following is a PDF corporate flow sample obtained by Threat Hunter from threat actors:

1.2 Fake bank app flow

Fake app flow refers to the copycat version of app software produced by threat actors according to the layout format of the official bank app. This type of copycat app involves mobile banking, third-party payment platform and other apps. Although it cannot conduct real transactions, it is highly simulated and can be operated.

Click to view and export functions related to accounts, transfers, transactions, etc. Some non-main function pages can only be displayed and cannot be clicked to enter lower-level pages. This type of copycat app involves mobile banking, WeChat, Alipay and other apps.

The following is the page information of a fake bank app:

1.2.1 Features of fake bank app

Bank apps faked by threat actors are independently developed based on official bank app styles, templates and some functions. In order to save the cost of counterfeiting, many apps lack internal functions and are easily discovered during manual verification.

Threat Hunter actually tested a fake bank app and found that the fake bank app has the following characteristics:

(1) The page functions related to turnover can be displayed normally and some functions can be operated normally, but real transactions are not possible.

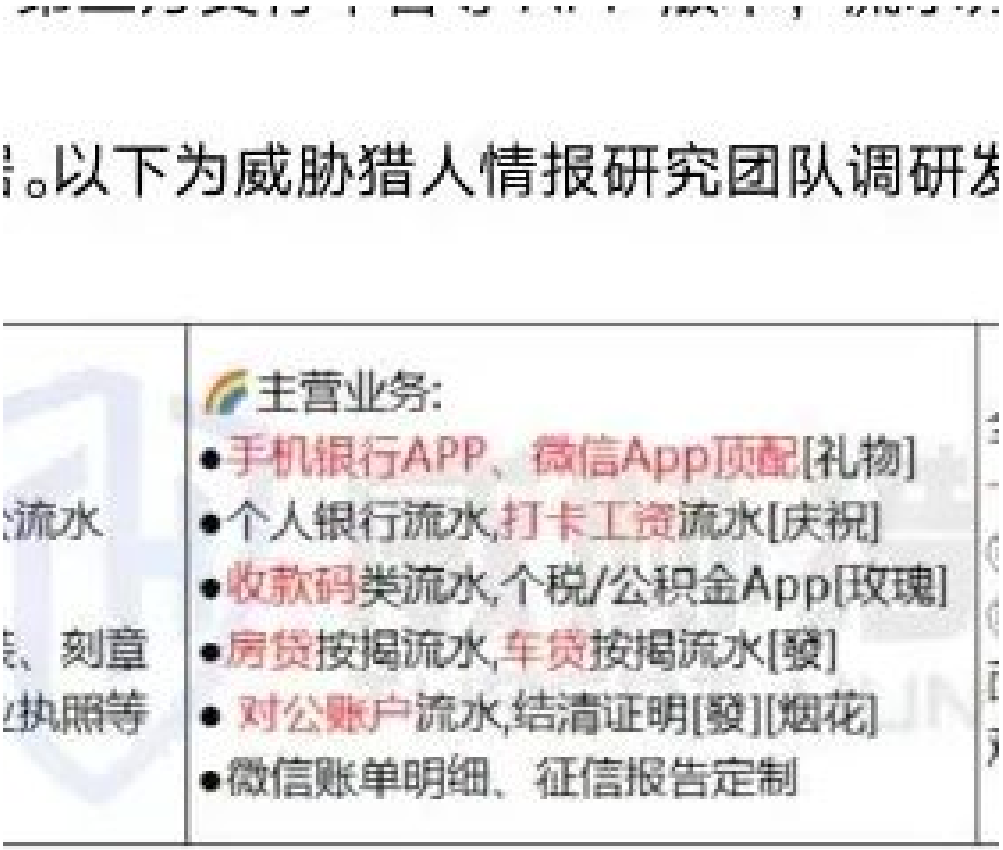
The fake bank app account inquiry function can click to enter the lower-level page and view the card number, view details, and enter the transfer page. The transfer and remittance function can also click to enter the lower-level page and view the transfer record and enter the transfer process. Click on the personal account of the common payee to enter the transfer page. The transfer process can be operated and the transfer will be displayed and the account balance will change in real time. Even if a fake bank account is used, the transfer will still be displayed as successful.

The following is the transfer record of a fake bank app:

(2) The regular first-level page menus on the main page that do not involve running water can be clicked normally to enter the lower-level pages, but the second-level menu pages cannot be opened, and the click is invalid. Clicking on the home page of the fake bank app for daily payment can enter the lower-level page, but all information on the second-level page is invalid when clicked, and the lower-level page cannot be opened.

(3) Non-main pages and other pages not related to running water only have display functions and cannot be clicked to open the page. The fake bank app homepage, pension and other modules cannot be clicked to open, and lower-level pages cannot be opened.

1.2.2 Fake bank app fraud process



Paper/PDF Streaming

Source: Threat Hunter original report, page 5

In actual fraud scenarios, threat actors generally gain profits by cooperating with financial intermediary channels. First, the intermediary evaluates the transaction data that the customer may need to supplement based on the customer's qualifications and loan needs. The threat actors create a detailed fake transaction data table based on the relevant requirements provided by the intermediary, such as the customer's false monthly income, false monthly expenses, false balance, transaction production cycle, basic customer information, etc., and import the transaction data into the background of the developed copycat version of the bank app to generate customer account information. Subsequently, the intermediary or client logs in to the customer account on the corresponding Shanzhai Bank app to view, display, and export the transaction data.

The above-mentioned generation process of false flow data can be completed by threat actors in just a few hours, and they can obtain illegal benefits ranging from a few hundred to several thousand yuan. threat actors provide false transaction services that formulate versions of various financial copycat apps. threat actors upload false transaction data in the background based on the false information provided by intermediaries. Financial intermediaries can use the fake transaction data by downloading and installing the copycat app through the software installation package provided by threat actors.

1.2.3 High and low app versions

Paper/PDF Stream (Chart 1)

Source: Threat Hunter original report, page 6

Paper/PDF Streaming (Chart 2)

Source: Threat Hunter original report, page 6

The mobile banking app is divided into two versions: low-profile app and high-profile app. The functions displayed on the high-profile app and the low-profile app are basically the same, and both are made according to the official banking app format and layout. The main difference lies in whether the mailbox can be exported and whether "transfer" can be done.

(1) Low-profile mobile banking app: You can only view the data in the app. The app production effect is relatively rough. It displays personal account information, account overview, income and expenditure details, transfer page and other information. It can display the data to the staff for verification or take a screenshot to retain the certificate during the interview. The price ranges from 500-600 yuan.

(2) Mobile banking high-end app: Not only can you view the data in the app, the app creates a more realistic effect. In addition to displaying personal account information, account overview, income and expenditure details, transfer pages and other information, it also has the function of exporting mailboxes and "fake transfers". You can freely choose to export the transaction data within a certain time period to the mailbox for printing. Customers can export the data on the spot during the loan interview and output it to the interviewer. The price ranges from 1,200-2,000 yuan.

The high-end version of the bank app exports the email address without entering the mobile phone verification code or entering the verification code at will to verify successfully, and the sender's email address is deliberately set to be very similar to the real official email address, so you need to check the difference carefully.

In addition, both high-end and low-end apps are suitable for Android mobile systems, and no cases of fake banking apps have been found on iOS systems.

1.3 Official bank app false statements

The fake transaction of the official bank app is that the black intermediary uses a specific mobile phone and flashes it to evade the anti-monitoring of the bank app, then installs the designated plug-in software provided by threat actors, and then downloads the official bank app. The threat actors use the remote control of the app to upload transaction data and generate false transactions in the mobile app. Black intermediaries apply for loans for customers by forging transaction data on the official app, increasing the approval rate and loan amount, and solving the problem of insufficient real transaction data for customers.

After the mobile phone device is flashed and fraud plug-ins are installed, the bank's official app is modified. Generally, the modification characteristics cannot be identified with the naked eye. However, it can be found through technical analysis that some functions of the official app may have been tampered with.

Through analysis, Threat Hunter learned that the technical operation process of official bank app’s fake transaction is as follows:

1 Flash the mobile phone device.

2 Install APatch to bypass Root detection.

3 Install Lsposed as Hook framework.

4. Install the Lsposed plug-in, which is used for hook bank app flow display related functions to display false flow in the app.

Technical logic: After the device obtains Root, the detection of the device environment by the bank app can be bypassed to a certain extent.

Lsposed is a feature-rich Hook framework. cybercriminal groups develops plug-ins based on this framework, which can hijack part of the bank app code without modifying the bank app. In this scenario, the cybercrime ecosystem may reversely locate the code for "getting the flow". Through the Lsposed framework, the return value of the code can be forcibly modified, that is, the fake flow data, thereby achieving fake flow display.

The following is the logical flow of threat actors hijacking the official bank app to display false transactions:

It is important to note that this kind of flashing of the phone and installing the plug-in will not affect the use of other functions. threat actors install plug-ins and remotely control the official bank app on the mobile phone. This app is completely real and all app functions can be used normally. Once this process is completed, you only need to change the customer's bank account and upload the false flow data table corresponding to the customer for reuse, but these data can only be displayed on that specific mobile phone.

Fake flow application scenarios

False bank app feature

Source: Threat Hunter original report, page 7

2. Fake flow application scenarios

False transaction statements may be used by threat actors in any loan product that requires verification of personal income level to assess repayment ability, but has not verified or cannot verify third-party official interface data. Home loans, car loans, etc. involving interview links are key attack scenarios for threat actors. Other loan scenarios such as bank statements (individuals and enterprises) failing to connect to bank data, personal tax data failing to connect to official tax center data, provident fund statements failing to connect to official data, etc. Loan scenarios that only rely on relevant mobile phone app data may have the risk of false transaction attacks.

2.1 Mortgage scenario

In home purchase mortgage loans and mortgage loan scenarios, it is often necessary to verify customer assets, social security provident funds, income statements and other materials. Customers are required to provide paper versions of income statements, check-in salary statements, or directly export data through bank apps. Such scenarios may involve risks of false statement fraud and fraudulent loans.

2.2 Car loan scenario

In the car purchase mortgage loan scenario, it is often necessary to verify the customer's real estate, social security provident fund, income level, etc. The customer is required to provide a paper version of the income statement, check-in salary statement, or directly export the data through the bank app. There may also be risks of false statement fraud and fraudulent loans.

2.3 Enterprise loan scenario

In corporate loan scenarios such as merchant loans, turnover loans, farmer loans, business loans, etc., some financial institutions require enterprises to provide business statements or legal person statements to prove the business status of the company. If business flow is involved, threat actors export the customer's real business and personal flow data, and refer to the customer's real up-and-down lines to create flow information, so that the flow may be true or false, or may be completely false. Therefore, there may also be risks of false flow fraud and loan fraud in corporate loan scenarios.

2.4 Consumer loan scenario

In personal consumption loans, in order to ensure the authenticity of the client's work, many financial institutions connect to third-party official data, such as social security and provident fund official data. This avoids some fraud and is a scenario where false statements are rarely used. However, there are still some financial institutions that need to verify customers' income statements. In this scenario, there may also be risks of false statement fraud and fraudulent loans.

defensive ideas

False bank app Fraud Process (Chart 1)

Source: Threat Hunter original report, page 8

Fake bank app Fraud Process (Chart 2)

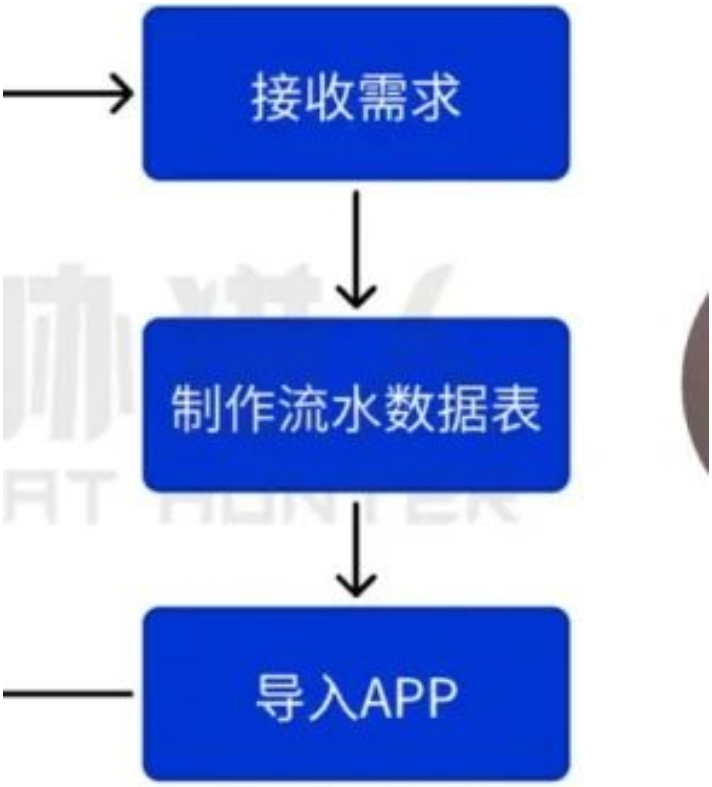
Source: Threat Hunter original report, page 8

3. Defense ideas

threat actors have different methods of operating fake transactions, and they are constantly iterating: from paper-based fake transactions, to fake bank app/third-party payment platform app low-end and high-end versions, to real bank official app transactions. The operating costs are getting higher and higher, and the packaging methods are more authentic and secretive. The attacks on financial institutions are constantly intensifying, and the fraud risks faced by financial institutions are more severe.

The Bank of Yamaya applies a false flow link (chart 1)

Source: Threat Hunter original report, page 9



The Bank of Shan is using a false water flow link (Chart 2)

Source: Threat Hunter original report, page 9

To this end, Threat Hunter provides the following suggestions for financial institutions in the direction of anti-fraud defense risks:

1. It is recommended to strengthen the risk training of counter-signing personnel on the characteristics of fake bank app transactions and synchronize the latest fake transactions in a timely manner.

Characteristics of cases and fraud techniques make interviewers always vigilant about the authenticity of bank app statements provided by loan customers.

2. It is recommended to strengthen the review of customer income flow data and conduct background checks and verification on large or abnormal transaction data.

The authenticity and reasonableness of the transaction.

3. It is recommended that users be required in user agreements and loan contracts to promise that the flow and transaction records provided are true and valid, and that the provisions are false.

Legal liability for false statements and warning of the legal consequences of forging false statements.

On the loan app side, Threat Hunter provides the following fraud controls suggestions from a technical perspective for the risk of tampering with bank official apps:

1. It is recommended to add xposed countermeasures, such as detecting whether the memory has been modified. Detect code snippets in memory and original code

Whether the fragments are consistent, if not, the current memory has been modified and may be hooked. Detect whether strings such as xposed and libepic exist in the so field in self_map. If they exist, it may be in an unsafe environment.

2. It is recommended to strengthen anti-debugging protection. Add more detection points to the Native layer and Java layer respectively, and distribute them to different animals.

In a static link library or class. By adding multiple confrontation positions, it increases the difficulty of analysis and delays the attacker's analysis process.

3. If it is detected that the device is in an abnormal environment, such as Root or Xposed, it is recommended to increase the risk score warning and add more people

Worker intervention risk review.

4. Summary

As a common means of credit fraud, false statements not only seriously disrupt the normal order of the financial market, but also greatly damage the interests of financial institutions and the trust of consumers. By forging or tampering with bank account transaction records, it bypasses fraud-control approvals, allowing applicants who do not meet the loan conditions to obtain funds, which may trigger a chain of financial risks, including an increase in non-performing rates, an increase in bad debts of financial institutions, and a threat to the stability of the entire economic system. Therefore, financial institutions need to continue to strengthen data verification and fraud controls in the credit approval process, improve the ability of technical means to identify false transactions, severely punish credit fraud, maintain financial security and stability, and protect consumer rights.

fraud plugins hijack the flow of water search and display links used by banks and present counterfeit data in real applications interfaces.

Source: Threat Hunter original report, page 10