Digital Fraud Wiki

Bust-Out Fraud

What is Bust-Out Fraud?

Bust-out fraud is a highly sophisticated, coordinated strategy that involves committing multiple acts of application fraud. Bust-out fraud is, in large part, orchestrated by organized crime rings. Which means financial institutions must be prepared for sophisticated bust-out fraud attacks at a massive scale. It is also a strategy that plays out over time, which makes it difficult to detect and significantly damaging for financial institutions.

A typical bust-out fraud attack involves a fraud ring applying for numerous credit lines using stolen or synthetic identities. Instead of maxing out the credit lines right away, the accounts exhibit behavior that mimic legitimate consumers. For example, the monthly payments for each account might be paid promptly for months, or even years. The fraud ring gradually builds good credit so that they can open as many credit lines at as many financial institutions as possible. When the time is right, all the credit lines are maxed out at once or within a short period. And all the lenders end up with numerous defaults and significant monetary losses.

What Should Financial Institutions Know About Bust-Out Fraud?

Fraudsters use automated tools such as bots and device emulators to create hundreds, even thousands of credit applications in a short amount of time. Automated tools allow bad actors to open

Loan Stacking

Synthetic Identity Theft

fraudulent credit lines at a speed and scale in which most financial institutions are ill-prepared to detect. And once the accounts are activated, device emulators allow fraudsters to evade detection by emulating legitimate borrower behavior.

Fraudsters use a variety of techniques so that they appear to be legitimate borrowers and to increase the chances that fraudulent credit applications will be approved. For example, a borrower with a high FICO score is likely to be approved for a new credit line by a lender. Some fraudsters steal identities that have high FICO scores to ensure that every fraudulent credit application they create is approved. Fraudsters also use synthetic identities to apply for lines of credit at many different banks. Synthetic identities are extremely difficult to detect and further the appearance that fraudulent applications are legitimate.

Bust-out fraud is a sophisticated, coordinated, and costly problem for every financial institution that provides credit services:

- Between 2003 and 2016, a fraud ring stole $200 million from banks through organized credit card fraud. The fraud ring created 7,000 identities, applied and was approved for 25,000 unique credit cards, which were mailed to 1,800 separate addresses. The fraudsters cultivated these accounts later busting them all out.
- Four defendants in the Central District of California were recently indicted for an alleged bust-out fraud scheme that resulted in nearly $2 million in fraudulent credit card charges. The defendants allegedly used synthetic identities and, in some cases, their real names to obtain numerous credit cards.

DataVisor Detects Bust-Out Fraud

To detect and defeat bust-out fraud, financial institutions must take a holistic approach to analyzing application attributes and linkable cross-account behaviors. Otherwise, they cannot hope to overcome the challenges posed by bust-out fraud. These challenges include:

1. Use of stolen or synthetic identities to create fraudulent accounts
2. Creation of fraudulent accounts that mimic genuine customer behaviors
3. Incubation of fraudulent accounts over time in preparation for malicious actions

Traditional detection systems are slow to react to fast-evolving bust-out fraud and cannot effectively differentiate good users from legitimate-seeming accounts that are, in fact, malicious.

This is why DataVisor created dCube, the revolutionary AI-powered fraud management solution—to capture synthetic identity and third-party fraud early, at the application stage, before damage can occur.

Through holistic data analysis, dCube's sophisticated models can reveal correlations and patterns that would otherwise go undetected; patterns that indicate coordinated malicious actions. By powering significantly higher detection accuracy and lower false positives, dCube enables businesses to continue creating frictionless customer experiences.

Additional References

Blog: Synthetic Identity Theft – When Credit Risk is Not Credit Risk

Solution: Application Fraud

Solution: Account Opening and Monitoring

Source: How fraudsters are gaming online lenders, American Banker

Source: Fourth Defendant Arrested in Credit Card 'Bust-Out' Scheme that Spent $2 Million on Luxury Watches, Liquor, Cars and Cemetery Plots, U.S. Attorney's Office, Central District of California

Source: Banks, Card Companies Seek Fraud Fix From Social Security Admin, Bloomberg BNA