Digital Fraud Wiki

Application Fraud

Background

Modern consumers want convenience. They expect financial institutions to provide digital products and services that are instant and available at any time. When consumers apply for lines of credit such as mortgage loans, car loans, and credit cards, they want the application and approval processes to be quick and easy. The consumer demand for convenience has led most banks to provide digital lending services with fast approval times.

Digital lending offers convenience for consumers but also opportunities for fraudsters to apply for loans and lines of credit on a grand scale. Fraudsters use tools like bots, virtual machines, and cloud infrastructure to initiate massive fraud application attacks against financial institutions. Fraudsters are creating hundreds, often thousands, of applications all at once through digital channels.

Fraudsters are also using sophisticated tools and techniques to emulate the behavior of legitimate borrowers, making their activities increasingly harder to detect.

What is Application Fraud?

Application fraud is where a bad actor uses a stolen or synthetic ID to apply for a loan or line of credit with no intention of paying back the lender. The fraudster gradually builds authentic-looking credit and account activity to gain access to more loans and higher lines of credit. Some fraudsters commit bust-out fraud, a broad strategy that

FRAUD DEFENSES

Crowdsourced Abuse Reporting
Device Fingerprinting
Email Reputation Service
IP Reputation Service
SR 11-7 Compliance
Supervised Machine Learning
Two-Factor Authentication (2FA)
Unsupervised Machine Learning

FRAUD TACTICS

Bot Attacks
Call Center Scams
Device Emulators
GPS Spoofing
P2P VPN Networks
Phishing Attacks
SIM Swap Fraud
URL Shortener Spam
Web Scraping

FRAUD TYPES

App Install Fraud
Application Fraud
Bust-Out Fraud

involves a fraudster committing multiple acts of application fraud. The fraudster cultivates numerous lines of credit over time. When the time is right, the fraudster maxes out all the credit lines in a short time frame and then disappears.

Avenues to Application Fraud

Fraudsters are clever, finding many channels that allow them to commit application fraud.

Data Breaches

Thanks to the more than 6 million data records lost or stolen every day fraudsters have a wealth of personal information at their disposal. Fraudsters use stolen personal data to create synthetic identities, impersonate customers, and take over accounts. Fraudsters also use stolen data for application fraud and techniques such as credential stuffing. Data breaches are the second biggest pain point leading to application fraud for financial institutions; first-party fraud is the top pain point.

Synthetic Identity Theft

Synthetic identity theft is a technique where a fraudster creates an identity either using a blend of personal information from different people, or a combination of real and fake personal information. Fraudsters swindle financial institutions out of billions of dollars every year by using synthetic identities for application fraud.

Call Center Attacks

Call centers are a prime target for fraudsters. According to Aite Group, 61% of fraud in the U.S. can be traced back to call centers. Many financial institutions allow consumers to apply for loans and lines of credit not only online but also by phone. Call center agents are unable to detect fraudsters using synthetic or stolen identities to complete loan or credit card applications, and traditional call center security measures are not designed to detect synthetic identities or coordinated fraud patterns.

Intercepted Mail

Some fraudsters are using stolen personal data and USPS Informed Delivery to apply for credit cards and then steal them directly from mailboxes. Informed Delivery is a service from USPS that allows users to preview mail and packages that are scheduled to be delivered. A fraudster can sign up for Informed Delivery using a different name and address. The fraudster is alerted as to when a credit card is scheduled to arrive at that address. The fraudster can then take the credit card from the mailbox before the owner has a chance to see it.

Scams Targeting Seniors

Scams that target potentially vulnerable groups such as senior citizens are among the top pain points related to application fraud for financial institutions. Fraudsters see senior citizens as being particularly susceptible to manipulation due to a perceived lack of technical knowledge, a heightened willingness to engage with seemingly plausible solicitations, and fewer opportunities to check with trusted sources before proffering private information.

Advanced Tools

Fraudsters have access to a wide array of tools to use for sophisticated application fraud attacks at massive scale.

Cloud Infrastructure

The same cloud services and infrastructure available to businesses are also available to fraudsters. Fraudsters purchase cloud computing services to run automated scripts and bots for massive fraud attacks.

Bots / Botnets

Fraudsters can use bots for a wide array of attack types. Bots can be used to generate variations of email addresses from common email domains such as Gmail and Outlook. Fraudsters also use bots to take over accounts via brute force hacking. A brute force attack is when a fraudster attempts to hack an account by entering various permutations of a password or PIN. Bots significantly speed up the process of brute force hacking attacks. Bots are also used for practices such as credential stuffing, in attacks on ticketing platforms, and more.

Virtual Machines

A virtual machine provides a virtualized interface to hardware like a CPU or RAM—it operates as a real computer and leverages CPU self-virtualization. Fraudsters can run applications on virtual machines for different operating systems like Windows, Android, iOS, and Linux.

Device Emulators

Device emulators are typically used by fraudsters to reset the Device IDs of mobile phones to avoid fingerprinting detections. Unlike virtual machines, emulators do not rely on CPU to run code directly—device hardware is emulated entirely in software.

Device Obfuscation

Device obfuscation refers to fraudsters utilizing mobile device flashing, virtual machines, or scripts to appear as though the login events of websites and mobile apps are coming from different devices.

IP Obfuscation

IP obfuscation refers to fraudsters using cloud services, virtual private networks (VPNs), or proxies to obfuscate IP addresses. IP obfuscation allows fraudsters to bypass IP blacklists and rules-based fraud prevention systems.

Location/GPS Spoofing

With the help of proxies, VPNs, or data centers, fraudsters can hide the real locations of devices—this technique is referred to as location spoofing.

Web Scraping Software

Scammers can find a wealth of personal data available online, especially on social networking sites. Fraudsters use web scrapers and data extraction software to extract personal information from web pages. The scraped personal information can be used as part of synthetic identities and to beat call center KBA questions.

Application Fraud Comes in Several Forms

Application fraud comes in many forms including demand deposit account application fraud, credit card application fraud, bust-out fraud, and first-party fraud.

Demand Deposit Account (DDA) Application Fraud

Fraudsters open and use DDA accounts to commit a variety of fraudulent attacks including check fraud, deposit fraud, and money laundering.

Credit Card Application Fraud

Fraudsters steal credit card numbers through means that include data breaches and malicious software. They also buy stolen credit card numbers from dark web marketplaces. However, sometimes fraudsters apply for credit cards directly, intending to max them out and never pay them back.

Bust-Out Fraud

Bust-out fraud is a type of fraud where a digital criminal uses stolen or synthetic identities to apply for loans and lines of credit over extended periods of time. The fraudster behaves like a legitimate consumer, building good credit and increasing the lines of credit. At a certain point, the fraudster maxes out the credit lines, drops the accounts, and then disappears.

First-Party Fraud

When the owner of the account commits the fraud, it is first-party fraud. A common form of first-party fraud is where an individual takes out a loan or line of credit with no intent to repay.

Tools Financial Institutions Are Using to Combat Application Fraud

Financial institutions approach application fraud on two fronts: call center security measures and online fraud prevention solutions.

Call Center Security Measures

Call center security measures often include a combination of knowledge-based authentication (KBA) questions, device intelligence, and phone number information. Call center representatives (CSRs) ask customers KBA questions such as “in what city were you born?” or “what is your pet’s name?” to confirm the caller’s identity. However, there are flaws with this strategy, as fraudsters can find much of the information needed to answer KBA questions on social networking sites, dark web marketplaces, or through social engineering.

Device fingerprinting, geolocation, and phone number information are often used by bank call centers to identify a customer at the beginning of a call. Device characteristics such as device ID, operating system, and browser version can be used to “fingerprint” the device. The financial institution uses the device fingerprint to identify customers who call the customer service center. However, these security measures are rarely enough to prevent an attack, as fraudsters often use tools to spoof device characteristics. As an additional security measure, some banks use a voice biometrics solution which analyzes the voice of the caller. The caller’s voice is compared to the voiceprint on file. Voice biometrics is problematic, however, because it is prone to false positives and increased error rates—voice patterns can change due to illness, emotional state, or aging.

Online Fraud Prevention Solutions

Some financial institutions use behavioral biometrics as a means of continuous authentication. Continuous authentication is where a user’s identity is verified throughout a session. Behavioral biometrics can help prevent many forms of fraud. However, modern fraudsters are finding ways to work around this approach as well.

Two-factor authentication (2FA) is another tool that financial institutions use to secure online accounts. When a user creates an account or logs into an existing account, a one-time passcode is sent to the user's phone, or a confirmation link is sent to their email. 2FA is used as a means of identity validation and to deter fraudsters. However, fraudsters have found ways to beat 2FA, including through automated phishing attacks.

Financial institutions also implement more sophisticated and technologically complex online fraud prevention solutions; the most common are rules engines, supervised learning (SML), and unsupervised learning (UML). On their own, each of these techniques can deliver a certain degree of value, although most fraud prevention techniques can lose effectiveness over time as fraudsters get access to better and cheaper tools to evade them, and none of these technologies is entirely foolproof.

For example, rules engines and rules-based systems are prone to false positives, and fraudsters can bypass rules easily. Supervised learning requires that new labels be continuously added to detect new and previously unknown fraud. Supervised learning-based systems are often not updated fast enough to catch new types of fraud. As to unsupervised machine learning, while it offers the greatest potential for preventing emerging fraud before damage occurs, it also requires advanced domain knowledge when used for specific use cases like fraud prevention. In some instances, UML algorithms are unable to scale to production level data sets, but an effective fraud prevention system requires scalability, speed, and adaptability.

Prevent Application Fraud with UML

Fraudsters are moving fast. They're leveraging advanced tools and employing complex approaches for their fraudulent applications. Traditional tools cannot keep pace when it comes to detecting emerging fraud, and comparatively modern solutions struggle as well. Behavioral biometrics and machine learning-based solutions can enhance detection coverage of application fraud, but also they're prone to generating high numbers of false positives.

With a mission to deliver proactive detection with unparalleled accuracy, DataVisor's team of fraud and data science experts have created dCube—the advanced fraud management solution powered by DataVisor's unsupervised machine learning (UML) technology—to defeat both known and unknown first-party, third-party, and synthetic fraud at scale.

While conventional rules or SML solutions require "pre-knowledge" of how attacks work to be effective, dCube is architected to detect fraud attacks without any historical labels, large datasets, or lengthy training time. Using dCube, financial institutions can adapt fast to emerging fraud without needing to anywhere from 6 to 12 months until their rules or SML models are updated.

Though fraudsters are using device obfuscation and cloud infrastructure to hide their footprints, dCube can capture even the slightest trace of their actions by taking a holistic approach to analyzing accounts and events while simultaneously performing trends and pattern analysis. On average, dCube delivers 20% detection lift and catches fraud at the application stage, which is usually two days to a week earlier than other solutions.

Learn how a leading U.S. credit card issuer uses DataVisor's machine learning solution to reduce application fraud losses.

Additional References

Blog: Emerging ATO Tactic: Call Center Scams – Part 1

Blog: How Call Center Fraud Leads to Account Takeover Fraud – Part 2

Blog: Mobile Fraud Gone in a (Device) Flash

Blog: Dealing with the Complexity of Fraud Attacks in Mobile Application Fraud

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

Blog: What Fraudsters Are Doing with Breached Data

Blog: Senate Bill 2155 Aims to Stop Synthetic Identity Fraud

E-Book: Guarding Your Online Marketplace Against Fraud

Solution: Application Fraud

Solution: Account Opening and Monitoring

Source: Synthetic Identity Fraud Cost Banks $6 Billion in 2016: Auriemma Consulting Group, Business Insider

Source: Application Fraud: Fighting an Uphill Battle, Aite Group

Source: 61% of Fraud Traced Back to the Contact Center, Pindrop (Aite Group)

Source: A new way to steal credit cards, Nextgov

Source: Hackers Beat Two-Factor Protection With Automated Phishing Attacks, PC Magazine

Source: Data Breaches: The Death Knell of KBA, Pindrop