“First-party fraud will be responsible for an estimated US $18.5 bn in credit losses for FIs around the globe in 2012, this is expected to grow to US $28.6 bn by 2016.”


This whitepaper discusses the challenges involved in combating first-party fraud and emerging best practice.

Banks can significantly reduce their levels of bad debt and collections expenses by specifically targeting first-party fraud. Advanced network analytics with real-time screening is the key to early detection and prevention of risk threats before they result in large losses.

WHAT IS FIRST-PARTY FRAUD?

First-party fraud covers a range of deceptive tactics used by fraudsters to obtain funds while masquerading as a genuine customer. These include:

- Unsecured credit — attempts by individuals or organized groups to establish unsecured lending facilities such as credit cards, loans or overdrafts with no intention to repay
- Secured products — for example where stolen checks are credited to a secured credit card
- Direct Deposit Account (DDA) — where the fraudster’s intent is to manipulate the float, usually using falsified deposits.

The true extent of this type of fraud is difficult to measure, especially where the fraudster’s financial profile is very similar to that of a good customer. As such, associated losses are often incorrectly written off as bad debt.
Fraudsters have developed well thought out approaches to commit first-party fraud comprising an entrance strategy to become onboarded as a customer, an escalation path to gain access to funds and an exit strategy to maximize fraudulent gains and evade detection. Typical methods include:

- stealing a real identity, where the unwilling victim is selectively targeted because of their good credit rating
- creating a synthetic identity which is either entirely fabricated, or comprises elements of real identities
- purchasing a real identity, for example from a temporary worker or foreign student who is departing
- creating a baseline credit bureau record using a synthetic identity to obtain services from utility providers
- manipulating lending policies using repeated applications to test for thresholds with the intention of creating an initial credit footprint in the bank
- spring-boarding from an account in good credit standing to obtain multiple additional products with a high combined value
- colluding with bank employees to circumvent the bank’s controls
- performing a bust-out using credit transfers, ATM withdrawals, purchase of goods that are easily resold or conversion to other financial instruments.

**ANATOMY OF A FIRST-PARTY FRAUD SCHEME**

**Stage 1 — Gaining entrance through fraudulent applications**

The fraudster applies for an account or product using details that have been purchased, stolen or manipulated. The objective is to get access to credit which would otherwise be denied. A key challenge faced by financial institutions is to identify application fraud while risk assessing a new-to-bank or ‘thin file’ customer where an accept/reject decision principally relies on data presented on the application form or retrieved from an external bureau rather than a full credit history.

The application fraud issue is compounded by the need to move the application process away from face-to-face channels in order to drive costs down, giving fraudsters the anonymity they need to create multiple accounts, test conventional rules and thresholds and develop an exploit strategy.

**Stage 2 — Escalating the value of a credit profile through sleeper fraud**

The fraudster will nurture a healthy credit profile for a period of time which can extend over many months. Account behavior is designed to mimic that of a good customer including regular direct debits; predictable inbound payments such as salary; normal bill payments and credit transfer patterns; on-time loan repayments; and no red flags in terms of debit or credit card transactions.

Techniques such as ‘cash-cycling’ are commonly used where funds are circulated amongst a ring of fraudulent accounts creating the illusion of legitimate transactional activity through the apparently normal credit transfer and repayment activity. However, these funds never leave the fraudster’s network.

The fraudster creates a credit rating which on the surface appears low-risk, and while undetected aims to accumulate lines of credit across cards, overdrafts and loans which when aggregated pose a significant loss exposure for the bank.

**Stage 3 — Successful exit and bust-out**

Having carefully built access to credit, the fraudster’s final aim is to exit the financial relationship while maximizing financial gain. Techniques involve credit transfers out of the jurisdiction; purchase of high-value goods on credit and debit cards; conversion to cash or writing bad checks. In addition, fraudsters will frequently be running tens or even hundreds of accounts and be operating with other fraudsters to maximize the bust-outs.
First-party fraud, especially where organized or involving some element of collusion, is not easy to discover. Why is this so?

**Knowledgeable adversaries**

Fraudsters have established supply chains that have evolved from buying and selling identities to the higher value activity of buying and selling information about the risk management controls deployed by financial institutions.

**Complex fraud rings designed to evade credit scoring models**

Sleeper fraud, involving well designed layers of accounts operated by clever fraudsters, is very hard to detect using the normal approach — standard methods rely heavily on score cards built at the customer level. The challenge is made even more difficult when the fraud ring crosses multiple financial institutions.

**Repeat offenders**

Predictive models built at the customer level can misclassify first-party fraud as bad debt. The longer term impact is that fraudsters are not characterized as having criminal intent and therefore retain access to the financial system, re-appearing in other guises at the same or different financial institution at a later time.

**Product silos**

Identifying first-party fraud is more challenging when the fraudster crosses various banking product lines. For example, fraudsters may obtain retail or commercial loans, which are subsequently used as a means of making regular payments for credit cards or for paying off small overdrafts, thus simulating healthy account behavior. Banks may be unable to detect these early indicators if their analytics and other controls are contained within specific lines of business.

**Insider involvement**

Organized fraudsters will typically buy, steal or create multiple identities which are used to create multiple customer relationships with substantial credit lines. Collusion with a bank employee enables higher-value attacks to be performed.
A MULTI-LAYERED APPROACH TO MANAGE FIRST-PARTY FRAUD

To tackle first-party fraud a financial institution needs to employ a multi-layered approach which disrupts fraudsters at all stages in their illegal schemes. Multiple lines of defense combining application screening, periodic reviews and real-time controls greatly diminishes the return on the investment required by the fraudster to obtain an identity, build a credit profile and achieve bust-out.

**Prevent fraud at the entry point**

Fraud prevention starts with customer onboarding, by creating a single customer view that combines information from all new applicants with all existing customers, financial institutions are then able to screen applicants before they enter the customer base. This is more effective than treating each new customer in isolation where personal details may have been altered or fabricated to avoid detection of single fraudulent applications.

Applications by an existing customer require the same level of scrutiny as for new customers especially where there is a change in circumstance such as new address, employer or personal relationship.

Accurate entity resolution is an important ingredient of the fraud prevention strategy — joining up disparate applications which originate from one fraudster or an organized group.

Furthermore, having the ability to make an immediate connection between a new applicant and any associates who already have an existing relationship with the bank is a valuable asset in disrupting fraud rings at the application stage.

**Proactive reviews to uncover sleeper fraud and collusion**

Fraudsters can evade the application screening process, especially where the identity is stolen or purchased and related to a healthy credit score. But proactive account reviews can be very effective in eliminating sleeper fraud where the fraudster simulates normal activity to win trust and increase credit lines.

It is important that reviews radiate out from the customer to include a broader set of personal and transactional relationships that indicate likelihood of first-party fraud. Social network analysis is an advanced analytical technique that provides financial institutions with the ability to find relationships between accounts and customers or between customers and employees that would otherwise be unknown. Social networks provide the additional predictors that discriminate fraud from bad debt; they help address the problem of uncovering complex layered rings; and they pinpoint undisclosed relationships between customers and employees.

**Guard the exit**

Transaction monitoring tools should have the ability to react to bust-out as it happens. In practice, these tools are often tuned to look for behaviors that indicate third-party account takeover. Even when velocity checks flag unusual transaction patterns, the fraudster can be prepared with a convincing explanation when contacted by their financial institution. Guarding the exit requires bridging the gap between application and first-party controls and transaction monitoring tools.
We deliver solutions which help our clients to protect and enhance their critical assets in the intelligence age. Our intelligent protection solutions combine large-scale data exploitation, ‘intelligence-grade’ security and complex services and solutions integration.

We operate in four key domains of expertise: cyber security, financial crime, communications intelligence and digital transformation.

Leading enterprises and government departments use our solutions to protect and enhance their physical infrastructure, mission-critical systems, valuable intellectual property, corporate information, reputation and customer relationships, competitive advantage and financial success.

We are part of BAE Systems, a global defense, aerospace and security company with approximately 90,000 employees. BAE Systems delivers a full range of products and services for air, land and naval forces, as well as advanced electronics, security, information technology solutions and customer support services.