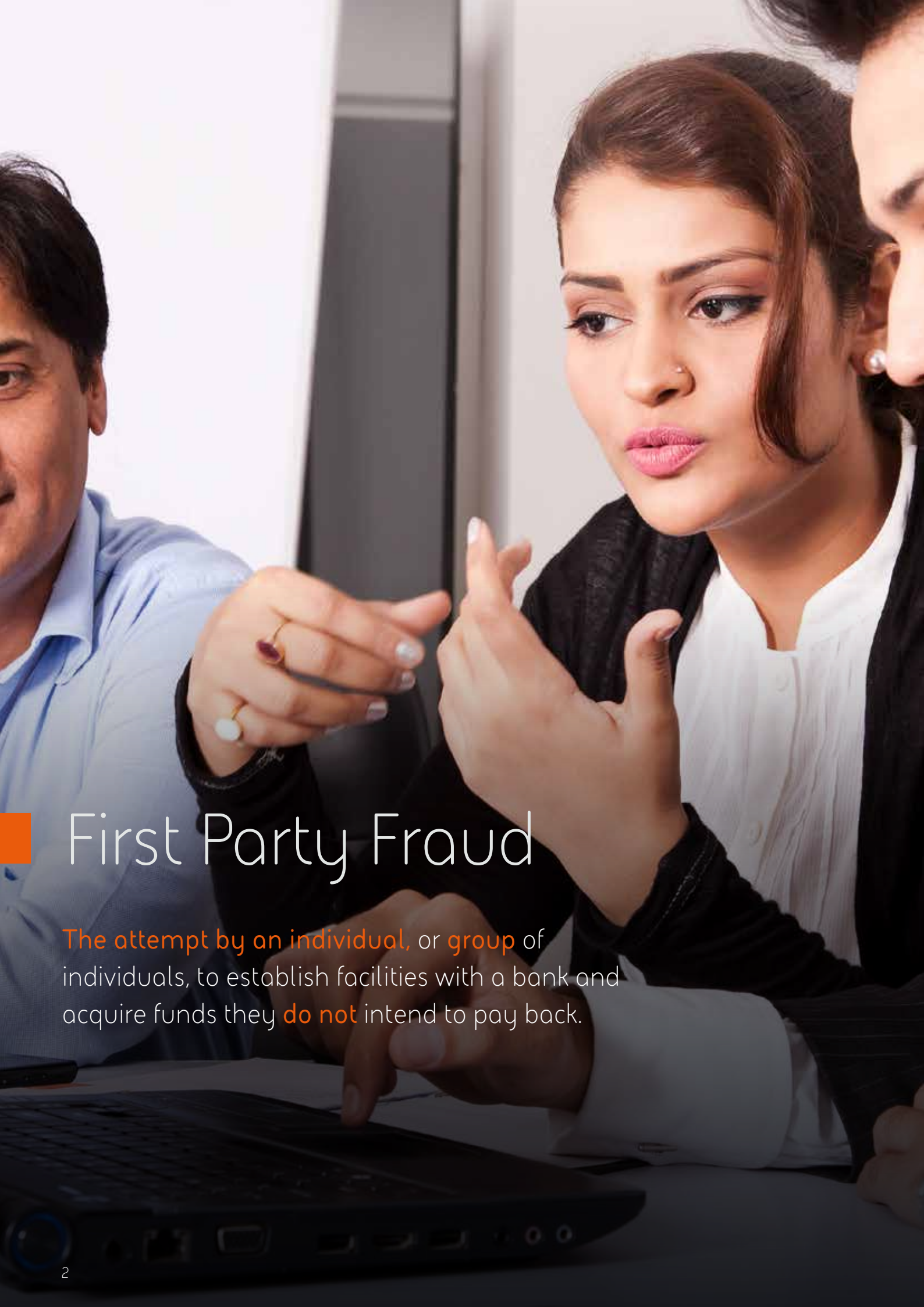
BAE SYSTEMS

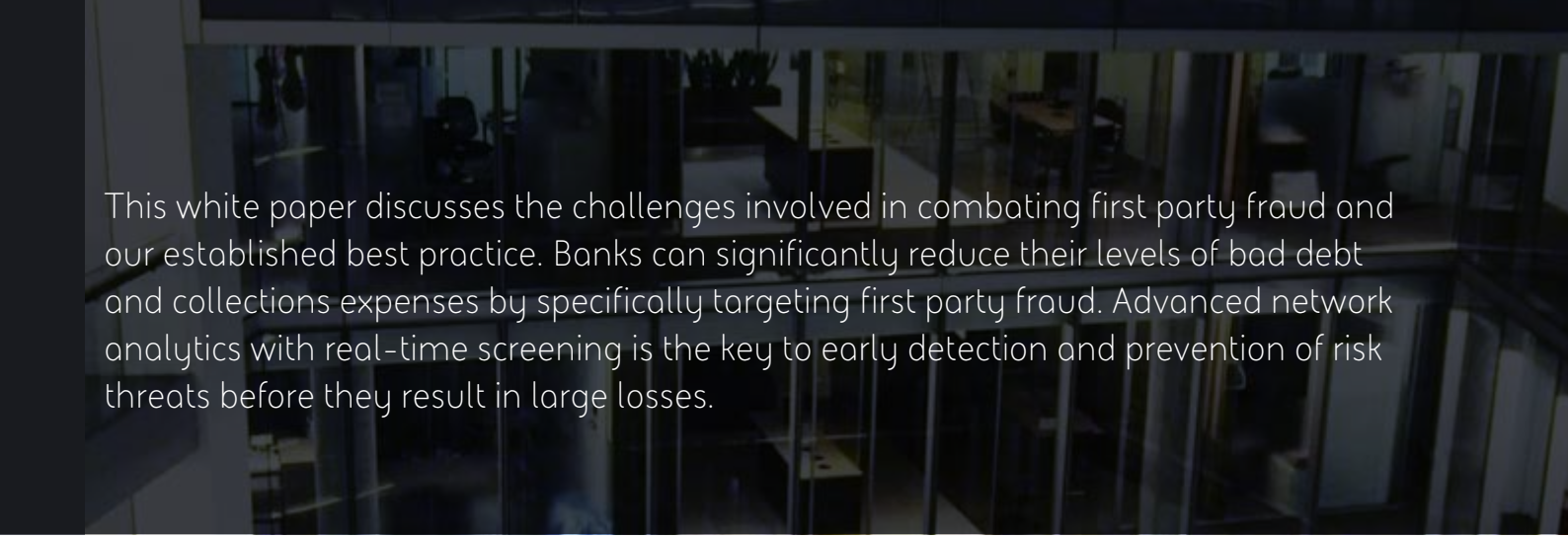
# Application Fraud and Account Monitoring

## A Holistic Approach to First Party Fraud



# First Party Fraud

The attempt by an individual, or group of individuals, to establish facilities with a bank and acquire funds they do not intend to pay back.



This white paper discusses the challenges involved in combating first party fraud and our established 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.

## Understanding and Managing First Party Fraud

Wherever merchants, lenders, service providers, government agencies or other organisations offer goods, services or anything of value to the public, they incur risk.

These risks include:

- **Credit risk -** arises when an individual receives goods or services in exchange for a promise of future repayment. If the individual's circumstances change in a way that prevents them from making the payment as agreed, the provider may not receive full payment and will incur a loss. Lender risk includes lost principle and interest, disruption to cash flow, and increased collection costs.

- **Fraud risk -** arises when the recipient uses deception to obtain goods or services. The type of deception can involve a wide range of tactics. Many involve receiving the goods or services while attributing the responsibility for repayment to someone else.

The difference between credit risk and fraud risk is intent. Credit risk usually involves customers who received the goods or services with a genuine intent on repaying the debt but lack sufficient resources to meet their obligation. Fraud risk starts with the intent to receive the goods or services without the intent to repay on the debt.

Between credit risk and fraud risk is a hybrid risk referred to as first party fraud risk. It includes elements of both credit and fraud risk. First party fraud involves an individual who makes a promise of future repayment in exchange for goods or services without any intent on repaying the debt.

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 organised 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.

First party **fraud** is a growing and pervasive problem that is siphoning billions of dollars from **financial** institutions, **insurance** companies, and government agencies each year.

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 maximise 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

Fraudsters have **developed well thought** out approaches to commit first party fraud ...

# 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 behaviour 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 maximising 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 cheques. In addition, fraudsters will frequently be running tens or even hundreds of accounts and be operating with other fraudsters to maximise the bust-outs.

> The objective is to get access to credit

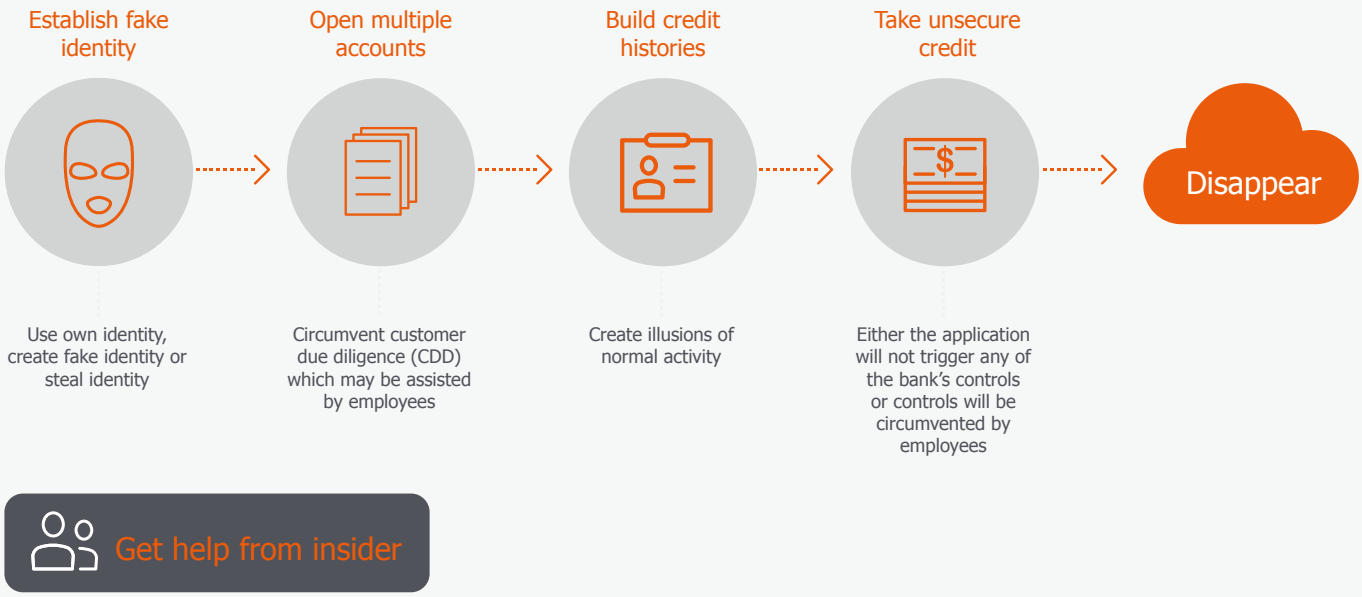



Figure 1. The first party fraud lifecycle

The **challenge** is made even more difficult when the fraud ring crosses **multiple** financial institutions

# Challenges in addressing first party fraud

First party fraud, especially where organised 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 characterised 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 behaviour. Banks may be unable to detect these early indicators if their analytics and other controls are contained within specific lines of business.

## Insider involvement

Organised 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.

## Playing the long game for best opportunity

Organised criminal groups will have multiple account activities across first party Fraud, Customer Scams, Mortgage Fraud and Mule Accounts. Having a detection platform that differentiates and optimally targets the different activities for investigators is key to being able to effectively execute fraud prevention.

# 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 organised 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.

Social networks provide the additional predictors that discriminate fraud from bad debt.

## Proactive reviews 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 the 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 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 behaviours 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.

# BAE Systems' Application Fraud and Account Monitoring solution

We are an expert provider of market proven financial crime analytics solutions to address the most complex industry fraud threats as well as offering major global banks, insurers, governments and law enforcement agencies our anti-money laundering and compliance solutions with top performing capabilities across the compliance lifecycle.

Our NetReveal solution provides an end-to-end capability for detecting, preventing, managing and reporting first party fraud. The solution prevents fraudsters from entering a financial institution's customer base by deploying the technology in real-time at the point of application and continuously monitoring customer behaviour before any bust-out occurs.

The network analysis platform differentiates positive customer activity, first party fraud and suspicious connections.

## Application screening

The NetReveal Application Fraud and Account Monitoring solution screens applications in real-time to provide an automated instant **accept** or **refer** decision. The detection process utilises information within the application, as well as related social networks and their associated risk to determine a level of identity fraud risk within the application. Signs of identity manipulation, distance from credit write-off and fraud, and evidence of organised hidden controls help to define network risk when screening applications. This approach proves successful in an environment where identity verification providers are challenged with the ability for customers to answer KBA questions and when much of the information is available for sale to fraudsters.

## On-going customer monitoring

NetReveal enables financial institutions to continually monitor accounts across deposit accounts and the entire lending book to find emerging risk of fraud. The first party fraud scoring process finds individuals or groups who are displaying the precursor behaviour that indicates intent not to pay. It applies social network analysis alongside a wide breadth and depth of analytical and machine learning techniques to investigate data across multiple channels and product lines.

## Advanced Analytical Detection

The NetReveal Application Fraud and Account Monitoring solution employs multiple detection techniques to efficiently find identity related fraud. The combination of Entity Resolution and Profiling, Social Network and Machine Learning Analytics allow for the identification of hidden and organised identity fraud schemes. These techniques are white-boxed to enable flexible changes and adaptations of fraud strategy over time with or without the assistance of BAE Systems analytical tuning resources.

New rules and models can be developed, tested and activated in real-time in order to give users flexibility to update their strategies

## Delivery Options

The NetReveal Application Fraud and Account Monitoring solution is available as an on premise deployed solution as well as a managed service offering. In the managed service offering, BAE Systems hosts and supports the data and environment to reduce IT overhead for financial institutions.

## Enterprise Fraud

The NetReveal Application Fraud and Account Monitoring solution forms part of an end-to-end retail and business banking fraud platform. Integrating application and first party fraud with solutions for real-time payments, deposit accounts, cards and insider fraud enabling a true enterprise view of customer fraud risk. Institutions across the globe are benefiting from this solution enabling them to more proactively and effectively manage their first party fraud losses.


- Screen all credit applications
- Application level scoring
- Risk-based approach to approve/reject
- Integrate within application process
  - Auto approval
  - Manual review of high-risk items

- Periodic review of relationship across product lines
- Customer level scoring
- Flag high risk customers for manual review and assessment

## We are BAE Systems

At BAE Systems, we provide some of the world's most advanced technology defence, aerospace and security solutions.

We employ a skilled workforce of 82,500 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, protect people and national security, and keep critical information and infrastructure secure.


**Global Headquarters**
**BAE Systems**
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

**BAE Systems**
265 Franklin Street
Boston
MA 02110
USA
T: +1 (617) 737 4170

**BAE Systems**
Level 12
20 Bridge Street
Sydney NSW 2000
Australia
T: +612 9240 4600

**BAE Systems**
Arjaan Office Tower
Suite 905
PO Box 500523
Dubai, U.A.E
T: +971 (0) 4 556 4700

**BAE Systems**
1 Raffles Place #42-01, Tower 1
Singapore 048616
Singapore
T: +65 6499 5000

BAE Systems, Surrey Research Park, Guildford
Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/businessdefence

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai


Victim of a cyber attack? Contact our emergency response team on:

US: 1 (800) 417-2155
UK: 0808 168 6647
Australia: 1800 825 411
International: +44 1483 817491
E: cyberresponse@baesystems.com

CREST CESG Certified Service Cyber Incident Response CPNI Centre for the Protection of National Infrastructure