BAE SYSTEMS

Learn about new banking fraud types and how to prevent them

Post-pandemic Outlook on Banking Fraud Prevention

Around the world, governments are currently spending big to prop up national economies quickly. In the US, the CARES Act has released around $2 trillion to businesses – the biggest rescue package the country has ever seen. Meanwhile in the UK, there are several initiatives which help SMEs access loans of up to £5 million, and similar schemes are in place across Europe and elsewhere.

This money is vital to taking the economic sting out of the current crisis, and has made financial institutions into the gatekeepers of much-needed government business loans.

The Challenge

Banks however have a responsibility to ensure only those deserving receive the funds they are entitled to or have their loan applications approved.

It is therefore important to understand the major fraud types likely to emerge over the coming months, and what can be done to minimise risk:

1. Classic shell company fraud. In some cases we are seeing classic shell company fraud attempts, where firms are created with the sole purpose of obtaining SMB loans. A recent example of this involved two businessmen from New England being charged for allegedly applying for over $500,000 in loans for businesses that weren't operating prior to the start of the pandemic, and which had no salaried employees[1].
2. Faking it for cash. Another involves business owners inflating the number of employees and the value of their salaries in order to extract more money. They could also lie about criminal records, fail to disclose liabilities or debts, alter tax returns, and engage in other fraudulent activity to secure access to all-important loans. This behaviour has resulted in recent arrests, with some high profile cases seeing business owners accused of spending millions of critical loan funds on themselves[2].
3. The professionals in action. Professional fraudsters (rather than real business owners) are also likely to make the most of current opportunities. Some may use phishing emails to harvest credentials and hijack business bank accounts in order to siphon funds away from the intended recipient. Meanwhile others may prefer to impersonate a legitimate business in loan applications, using forged documents with changed bank account details.

The Solution

Unfortunately, traditional fraud filters are not always set-up to deal with this potential surge in scam applications. But there are things financial institutions can do to protect themselves.

One of the best places to start is by reaching out to any government-level contacts for additional intelligence. This is arguably easier done in Europe than the US, where state and federal government siloes may cause extra delays. Things like employee count lists are not normally shared with banks, but datasets like these can go a long way to improving visibility into potential loan applicants. Now may be the time to reset some of those essential baseline profiles on which fraud models are built.

Fintech or fraud prevention players, which specialise in delivering intelligence feeds that profile what "normal" looks like, can also help banks to better spot suspicious activity. Link analysis capabilities, meanwhile, are useful in helping to join the dots between malicious activities, to uncover and predict future fraud.

Collaboration is also important inside banks. Risk and Compliance teams should be working closely with IT security so that any early warning signs of malicious behaviour are spotted and shared. The key here is to automate without losing accuracy or auditability. That means any workflow capability must be able to handle the large volume of applications coming in, and risk-based decisioning tools should be transparent in explaining why particular applications are rejected.

While we continue to work in challenging times, a bank's ability to spot fraud is becoming ever more crucial.

The BAE Systems Approach

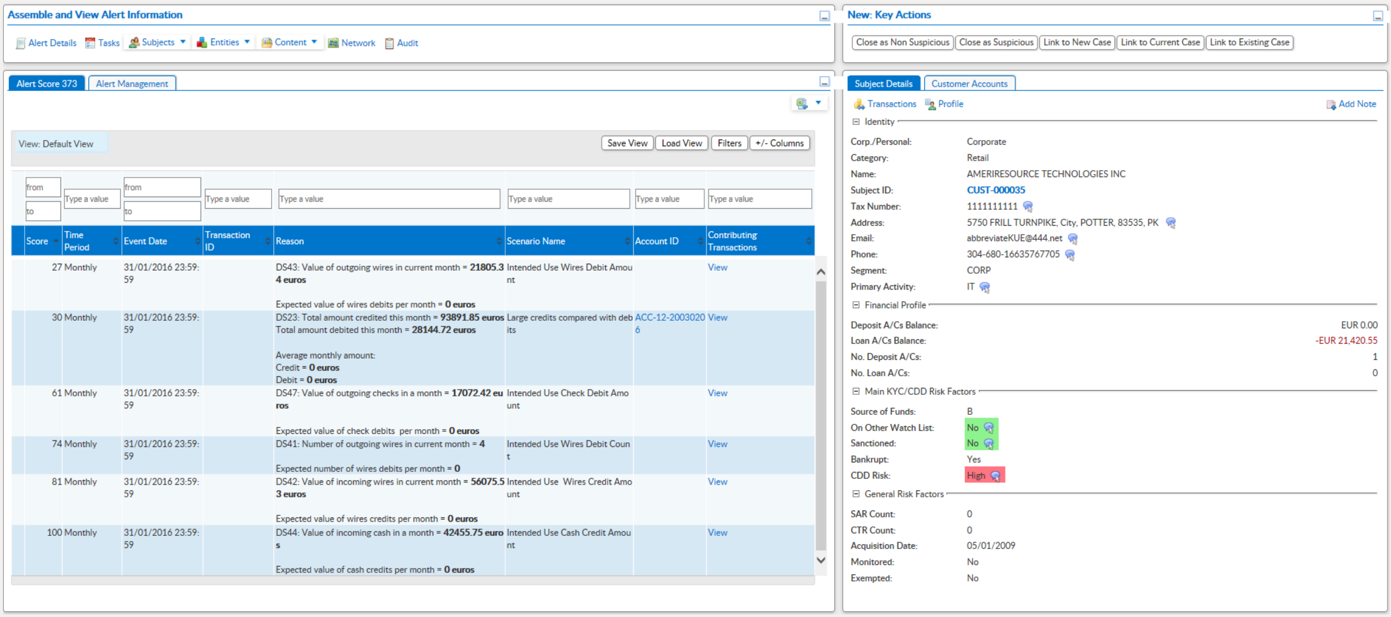
Tackle financial crime with an integrated approach to fraud and AML compliance

Our Capabilities

NetReveal® Case Management

Our solution spans the entire financial crime, risk, fraud and compliance functions. It is an open and flexible case management platform that efficiently organises data inputs (including third party data). It prioritises and centralises alerts and incidents into one enterprise-wide investigation platform to help manage investigations.

- Better collaboration – Consolidates related alerts, evidence and financial metrics into a single dossier. Closed cases are retained indefinitely or for as long as audit standards require.
- Increase effectiveness and efficiency – Aggregates risk indicators across source systems and presents a holistic view to analysts. Improve efficiency with users focussed on analysis rather than data gathering.
- Improved decision making – Investigation data is presented to investigation teams in a logical way, using instructional design techniques to simplify and accelerate decision making.



Score	Time Period	Event Date	Transaction ID	Reason	Scenario Name	Account ID	Contributing Transactions
27	Monthly	31/01/2016 23:59:59		DS43: Value of outgoing wires in current month = **21805.34 euros** Expected value of wires debits per month = **0 euros**	Intended Use Wires Debit Amount		View
30	Monthly	31/01/2016 23:59:59		DS23: Total amount credited this month = **93891.85 euros** Total amount debited this month = **28144.72 euros** Average monthly amount: Credit = **0 euros** Debit = **0 euros**	Large credits compared with debits	ACC-12-20030206	View
61	Monthly	31/01/2016 23:59:59		DS47: Value of outgoing checks in a month = **17072.42 euros** Expected value of check debits per month = **0 euros**	Intended Use Check Debit Amount		View
74	Monthly	31/01/2016 23:59:59		DS41: Number of outgoing wires in current month = **4** Expected number of wires debits per month = **0**	Intended Use Wires Debit Count		View
81	Monthly	31/01/2016 23:59:59		DS42: Value of incoming wires in current month = **56075.53 euros** Expected value of wires credits per month = **0 euros**	Intended Use Wires Credit Amount		View
100	Monthly	31/01/2016 23:59:59		DS44: Value of incoming cash in a month = **42455.75 euros** Expected value of cash credits per month = **0 euros**	Intended Use Cash Credit Amount		View

⊟ Identity

Corp./Personal:	Corporate
Category:	Retail
Name:	AMERIRESOURCE TECHNOLOGIES INC
Subject ID:	CUST-000035
Tax Number:	1111111111
Address:	5750 FRILL TURNPIKE, City, POTTER, 83535, PK
Email:	abbreviateKUE@444.net
Phone:	304-680-16635767705
Segment:	CORP
Primary Activity:	IT

⊟ Financial Profile

Deposit A/Cs Balance:	EUR 0.00
Loan A/Cs Balance:	-EUR 21,420.55
No. Deposit A/Cs:	1
No. Loan A/Cs:	0

⊟ Main KYC/CDD Risk Factors

Source of Funds:	B
On Other Watch List:	No
Sanctioned:	No
Bankrupt:	Yes
CDD Risk:	High

⊟ General Risk Factors

SAR Count:	0
CTR Count:	0
Acquisition Date:	05/01/2009
Monitored:	No
Exempted:	No

NetReveal EIM: Example alert screen

Benefits

NetReveal utilises robotic process automation (RPA) and other innovations that improve operational efficiency and transform the effectiveness of investigators and analysts. Features include:

- A single centralised 360-degree customer view, covering all pillars of compliance, consolidating customer associated information (e.g. KYC) with a fully audited trail of historical alert and case investigations. This central investigation source has improved efficiency by 30-40%, fostering intelligence-led alert and case disposition decisions.
- Advanced analytics with artificial intelligence and machine learning which operate in conjunction with existing detection logic to detect new criminal approaches and trends in AML and fraud.
- Real-time and batch connectivity to minimise potential risk to your organization.
- Profiling based on specific entity (e.g. account, customer, transaction), flexible segmentation and peer group, behavioral, and risk analysis.
- Componentised (or de-coupled) technology stack increases deployment flexibility and makes future upgrades easier.
- Auditability on decisions and actions that can be easily reviewed by line of business leads through to external auditors.

Why BAE Systems?

- We are trusted by more than 33% of global top 100 banks who use our solutions
- Our data science practitioners and subject matter experts boast years of deep domain and financial services experience.
- Our solutions provide a breadth of functionality: holistic single platform, white box detection, along with efficient and intuitive user interfaces.

SOURCES

[1] Source: USA Today, May 2020

[2] Source: WSBTV.com News, May 2020

BAE SYSTEMS

Contact Details: UK: +44 (0) 203 296 5900 | US: +1 800 234 2175 | AUS:+61 3 8623 4400 | SING:+65 6714 2100

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

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

linkedin.com/company/baesystemsai   twitter.com/baesystems_ai