# ARIC™ Scam Detect

*NEW!*

**Protection from day 1**

Authorised Push Payment scams are the fastest-growing fraud type, with investment scams rising by 193% in five years. For the top 200 U.S. financial institutions (FIs), scams were a quarter of fraudulent transactions, with average losses of over $100 million in 2021. In the U.K., losses during the first half of 2022 were £249.1 million.

The financial services industry has been working with Featurespace to find a solution to protect their organizations and their customers from losses. **ARIC™ Scam Detect from Featurespace is our response.**

---

**What are Authorised Push Payment scams?**

Authorised Push Payment (APP) scams occur when a customer is persuaded by a criminal into transferring money to an account the criminal controls. Scams target the customer to authenticate and authorize the payment. DeviceID or IP information will not help to improve detection and traditional fraud controls typically do not monitor inbound payments. Despite FIs ensuring the customer is genuine, once an APP scam is executed it is difficult to reverse or retrieve the funds.

**ARIC™ Scam Detect protects customers from scams in real time**

Powered by the best performing AI and machine learning models, ARIC™ Scam Detect uses real-time behavioral analytics to profile the customer and their interactions holistically, extracting more signals from payment data already available.

ARIC™ Scam Detect profiles both the inbound flow of funds, as well as spending patterns, and identifies customers who are moving funds (outbound) to make a scam payment or are acting as money mules.

The solution can be layered on top of existing controls to provide additional protection. Financial institutions can now improve management and tracking of scams overall.

**Entities profiled in Authorised Push Payment scams (examples):**

<table>
<thead>
<tr>
<th>Scam Type</th>
<th>Entity Profiled</th>
<th>Indicator of scam examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impersonation Scam</td>
<td>New or changed beneficiary</td>
<td></td>
</tr>
<tr>
<td>Romance Scam</td>
<td>Beneficiary and Victim</td>
<td>Gradually increasing payments</td>
</tr>
<tr>
<td>Investor Scam</td>
<td>Multiple payments, typically increasing in value</td>
<td></td>
</tr>
</tbody>
</table>

---

1. Source: Investment scam reports rise by 193% in five years, Financial Times, 21 February 2023
3. Source: UK Finance, 2022 Half Year Fraud Update
How does ARIC™ Scam Detect work?

ARIC™ Scam Detect features:
- Pre-configured behavioral models with scam coverage from day one
- Score augmentation or ARIC™ Risk Hub
- Real-time inbound and outbound payment monitoring and profiling for comprehensive protection
- Support and maintenance

Technical specification:
- Hosted on Featurespace cloud
- Secure, SOC-2 compliant and encrypted platform
- Ingest payment data in ISO 20022 schemas
- Integration via API
- No historic data required
- Fewer than 30 data attributes required

Pricing calculated based on transaction volumes. Contact us at info@featurespace.com