How UK Building Societies Can Detect Fraud Without Compromising Member Experience

UK Building Societies are mutual financial institutions that provide banking services like savings accounts, mortgages, and loans in the United Kingdom. Unlike banks, these institutions are owned by their members rather than shareholders. This allows them to focus on community-driven financial services while strongly emphasizing trust, security, and customer well-being.

The rising threat of fraud in UK Building Societies

Building Societies are a cornerstone of financial security for millions of UK residents and, as member-owned institutions, maintaining trust is paramount. However, fraudsters are evolving, using increasingly sophisticated tactics to infiltrate phone and digital banking channels. Cyber threats continue to rise, and with fraud losses in the UK **exceeding £571 million** in the first six months of 2024 (increasing **19% compared to 2023**[1]), proactive fraud mitigation is essential.

Key takeaways:

▌ UK Building Societies face increasing fraud risks from APP scams, account takeovers, impersonation fraud, and phone-based scams.

▌ Traditional security measures like passwords, PINs, and security questions are no longer sufficient.

▌ Pindrop® Solutions provide proactive fraud detection tools for voice, device, and behavior analysis.

▌ Enhance security and customer trust without compromising member experience.

Statistics:

▌ Fraud losses in the UK **exceeded £571 million** in the first six months of 2024[2]

▌ The UK saw a **19% increase in fraud cases** and **7% increase in losses** compared to 2023[3]

▌ Pindrop® Protect's advanced risk analysis surpasses traditional tools, with a **fraud detection rate of up to 80%**[4]

---

[1] https://www.ukfinance.org.uk/system/files/2024-10/Half%20Year%20Fraud%20Report%202024.pdf

[2] https://www.ukfinance.org.uk/system/files/2024-10/Half%20Year%20Fraud%20Report%202024.pdf

[3] https://www.ukfinance.org.uk/system/files/2024-10/Half%20Year%20Fraud%20Report%202024.pdf

[4] Fraud detection rate calculated as fraud detected by Protect as proportion of all confirmed fraud calls across all Pindrop® Protect customers for the full year 2023.

Top fraud risks facing Building Societies

Authorised push payment (APP) scams – Criminals impersonate trusted institutions to trick members into transferring money to fraudulent accounts. Building Societies are particularly vulnerable as they prioritize customer trust and service, but preventing fraud is challenging because transactions are authorised by the customer, limiting the ability to block fraudulent payments without undermining user autonomy.

Account takeover (ATO) – Fraudsters gain unauthorized access to a customer's account—often through phishing, malware, or leaked credentials—allowing them to make fraudulent transactions or change account details.

Impersonation fraud – Criminals posing as trusted individuals or organizations, such as bank representatives or government officials, manipulate customers into revealing sensitive information or authorizing fraudulent payments. Building Societies face challenges in detecting this fraud, as criminals exploit social engineering tactics to bypass security measures, putting both members' funds and institutional credibility at risk.

Vishing and phone-based fraud – Fraudsters use phone calls to deceive customers into revealing sensitive information or authorizing fraudulent transactions, often by impersonating banks, government agencies, or tech support. Building Society members may trust a caller claiming to be from their institution, making it difficult to distinguish legitimate contact from sophisticated scammers.

First-party fraud – An individual deliberately misrepresents their identity, financial situation, or intentions to obtain credit, loans, or other financial benefits, often with no intention of repayment. In this case, the fraudster is the actual account holder, making detection difficult for Building Societies as the accounts initially appear legitimate.

Insider threats and compliance risks – Building Societies must navigate protecting against internal fraud, including employees misusing their access to customer accounts or confidential data for financial gain, while complying with **Financial Conduct Authority (FCA)** and **Prudential Regulation Authority (PRA)** regulations.

The urgent need for advanced security solutions

As cybercriminals evolve, traditional security measures—like passwords and security questions—are often no longer enough. Customers expect convenient, frictionless access to their accounts online or over the phone, and overly complicated authentication processes may be frustrating. Building Societies need integrated security and authentication solutions to help protect members from fraudsters while maintaining seamless banking experiences.

How Pindrop® Solutions benefit UK Building Societies

Detecting fraud early

With fraudsters constantly evolving their tactics, Building Societies need to **spot fraud in real time**, rather than responding after financial losses occur.

▐ Proactively detect and block suspicious callers before they can scam members using **Pindrop® Protect**, which analyzes **behavioral patterns, call metadata, and voice characteristics** to identify fraud risks.

▐ Stop account **takeovers and APP scams** by catching fraudsters that are using deepfake voices, spoofed calls, and synthetic identities—leveraging **risk analysis** that detects anomalies that are easy-to-miss for human agents with Pindrop® Protect and Pindrop® Pulse.

▐ **Reduce fraud-related financial losses**, helping protect both members and operational revenue.

Frictionless member authentication that builds trust

Security questions, one-time passcodes, and long authentication processes can frustrate members while still leaving them vulnerable to social engineering scams. **Building Societies need a faster, more secure way to verify members**.

▐ **Authenticate members** with **Pindrop® Passport**, reducing reliance on PINs, passwords, and personal details.

▐ **Reduce call center wait times** by **removing manual authentication steps**, so agents can focus on service instead of security challenges.

▐ **Enhance the member experience** by allowing customers to verify their identity naturally, even when calling from a new device or location.

Defend against advanced fraud attacks in digital and phone banking

As Building Societies expand their digital and phone-based services, fraudsters are finding new ways to **exploit vulnerabilities in remote banking channels.**

▐ **Secure phone interactions, even before a member speaks,** by using **Pindrop® Protect**, which analyses background noise, device signals, and call metadata.

▐ **Pindrop® Protect leverages our fraud consortium**, a proprietary database of confirmed fraudsters, accumulated through 12+ years of intelligence.

▐ **Maintain a seamless omnichannel experience**, allowing members to **access services securely via phone, mobile, and web banking**, without additional friction.

Improve operational efficiency and reduce costs

Fraud investigations, manual authentication processes, and false positives drain resources and increase costs for Building Societies.

▮ **Free up customer service teams** by automating authentication, in some cases reducing verification time by up to 50%.[5]

▮ **Minimize fraud-related costs** by stopping high-risk transactions before they happen, helping to reduce financial exposure to APP scams, impersonation fraud, and account takeovers.

▮ **Improve fraud detection accuracy**, helping reduce the number of false positives that unnecessarily block legitimate members.

Maintain compliance while strengthening your institution's reputation

Many Building Societies are looking for ways to **proactively defend against fraud** while maintaining high service standards, including:

▮ **Meeting FCA and PRA requirements**, in part by implementing fraud detection that actively works to catch financial crime attempts.

▮ **Protecting their reputation as a safe, ethical financial institution**, reinforcing member trust and confidence.

▮ **Staying ahead of evolving fraud tactics** by leveraging **fraud detection that continuously learns and adapts** to new threats.

Why now? The future of fraud detection for UK Building Societies

Fraudsters are leveraging AI, deepfake voices, and social engineering tactics at an increasing rate, making traditional security solutions obsolete.

▮ **Fraud attacks are becoming AI-powered** – Deepfake voices and synthetic speech are making it easier for fraudsters to bypass legacy authentication methods.

▮ **Fraud losses are rising**, and financial institutions must act now.

▮ **Members expect seamless security** – Call center hold times, frustrating authentication, and OTP fatigue drive dissatisfaction.

▮ **Scrutiny is increasing** – Institutions must prove they are taking proactive steps to detect fraud.

Pindrop provides security solutions that meet these challenges head-on, helping UK Building Societies stay focused on security and member experience.

Find out how Pindrop solutions can transform your fraud detection strategy for your Building Society.
Get in touch today to request a demo.

---

[5] https://www.pindrop.com/research/case-study/michigan-state-university-federal-credit-union/

pindrop.com | info@pindrop.com