The Digital Front Lines

How Banks and Telecoms Can Unite Against Fraud

Fraudsters are becoming increasingly innovative in their methods to approach and manipulate their targets. With the spread of technologies like AI tools and the growth of globalization, fraud groups move faster and develop more effective ways to commit crimes, especially when combining multiple technologies. As a result, there is pressure for mutual cooperation across sectors. Industries are becoming interconnected, and although they still provide different services, technological progress connects these services, and they practically cannot function without each other. This connectivity is clearly seen in the financial services and telecommunications industries. The use of two-factor authentication via SMS codes or accessing internet banking through smartphone applications, for instance, has become people's daily routine. Undeniably, the connection between financial services (FS) firms and telecommunications companies will become more significant in the future, making it crucial for those two industries to identify synergies for cooperation.

Forms of phishing and “APP” fraud are infiltrating our smartphones, putting our finances at risk

The evolution in mobile technologies has led to more sophisticated methods of committing digital fraud. Outlined below are some of the most common types of frauds representing an abuse of services FS firms and telecoms offer:

Phishing

This fraud has been a well-known threat for nearly three decades, but its popularity has risen in recent years. It often starts with a simple phishing SMS (“smishing”) that tricks a person into clicking on a harmful link, leading to a loss of control over their smartphone by involuntary malware installation in the background.

SIM Swap Fraud

This involves hijacking a SIM card to receive SMS messages or calls. Fraudsters use this technique to access accounts that require two-factor authentication. Then they purport to be the victim attempting to make changes with their bank or mobile provider to steal the genuine customer’s mobile identity.

Authorized Pushed Payment (“APP”) scams

In these scams, a person is misled to voluntarily make a payment, often as a matter of urgency, to a fraudulent beneficiary, for what they believe is a genuine service or product. Fraudsters use phone calls or WhatsApp to reach victims, often combining these with AI tools with face manipulation apps and conversation automation to make their scams more effective. Whether it is a fake romance scam, someone pretending to be a close relative or supervisor at work, or offering “the best opportunity to invest,” fraudsters are persuasive.

Voice over IP (“VoIP”) frauds

VoIP frauds usually happen when fraudsters use internet-based phone systems to fake their caller ID. Fraudsters disguise their identity, pretending to call or write from a bank or another reputable institution. They trick targets into clicking on malicious links, disclosing personal data or sending money.

These are just some examples of how fraudsters operate today to gain as much as their target can offer without them even knowing it. To prevent these frauds, FS firms and telecoms must stay vigilant by not only securing their systems but also raising customer fraud awareness amongst both their customers and employees.

Cooperation as today’s must

Cooperation between FS firms and telecoms could make a big difference in tackling fraud and a great example comes from the Global Anti-Scam Alliance (“GASA”) which aims to create a world where people worldwide are safe from the financial and emotional trauma caused by online scams. They work towards this goal by bringing together industries targeted by fraudsters, such as FS firms and telecoms, to share knowledge and best practices, hosting regular events where experts share their insights on tackling online scams.

A notable example of fighting crime together is the initiative launched in Great Britain by the GSM Association and UK Finance. Due to the high number of APP scams, they joined forces in 2024 to combat fraud by sharing an Application Programming Interface (“API”) called “Scam Signal”. This was made possible thanks to project CAMARA, which is laying the groundwork for a global fight against fraud. Initially developed to facilitate and standardize the integration of APIs in the telecommunications sector, CAMARA is increasingly relevant as banking and telecommunications converge. Implementing these APIs into banking systems can significantly enhance fraud detection and prevention efforts.

Another excellent example of such cooperation is the one between the Bankers Association of the Philippines and Ayala-led Globe Telecoms Inc. The two organizations have formed an intelligence-sharing network to combat cybercrime, including phishing, identity theft and fraudulent SMS messages. This ongoing collaboration involves sharing information on the latest cybersecurity threats and helping banks develop effective countermeasures. In addition to industry good practices of collaboration, regulators are becoming increasingly more active in bringing the FS and telecommunications industries together.

In response to rising phishing scams, Singapore recently introduced the Shared Responsibility Framework (SRF), announced by the Monetary Authority of Singapore (MAS) and the Infocomm Media Development Authority (IMDA) on 24 October 2024. Beginning 16 December 2024, financial institutions and telecoms providers must follow specific guidelines to avoid liability for phishing-related losses. These include a 12-hour cooling-off period after activating a digital security token and real-time notifications for high-risk activities. Institutions must also implement 24/7 reporting channels, fraud surveillance, and self-service features to block unauthorized account access. In determining who is liable for a fraud loss in an incident, an initial check is performed as to whether the payment services provider had applied appropriate measures to prevent the incident, after which the telecommunications provider’s controls are put under scrutiny. The customer is only liable if both institutions have applied adequate controls to prevent the fraud.

The Australian government is following MAS’s lead by introducing new legislation aimed at reducing scams, holding banks, telecoms, and digital platforms responsible for malicious activities on their networks. Under the Scams Prevention Framework, these sectors must implement measures to prevent scammers from reaching Australian residents, with severe penalties for non-compliance. Banks are tasked with verifying payees to ensure transparency in financial transactions, while telecoms must detect and disrupt scam calls and messages. In addition to the Scam Prevention Framework, Australia introduced another significant initiative: an anti-scam intelligence loop. This initiative unites banks, telecommunications networks, internet service providers, and social media companies to enhance defenses through shared intelligence. Co-designed by the Australian Financial Crimes Exchange (AFCX) and the National Anti-Scam Centre (NASC), the initiative enables these organizations to quickly exchange verified data, allowing for faster action against scams. This includes blocking fraudulent phone numbers and URLs, as well as removing fake websites and social media posts.

The examples above are seen as industry good practice on how FS firms and telecoms can collaborate to fight fraud. The ever-evolving and expanding nature of fraud will hopefully drive the launch of cooperation at various levels worldwide, involving not just cross-sector businesses but also more non-governmental and state organizations to help in prevention.

Putting the customer first

Telecoms, with their advanced fraud detection systems for call data, can offer insights into technical tools for verifying user identities or preventing unauthorized access, which FS firms could adapt for banking transactions. Similarly, financial institutions, with their anti-fraud algorithms, could inspire telecom companies to adopt similar tools to track and prevent fraudulent behavior on their side. Additionally, sharing information on internal fraud-related policies could help both sectors improve their overall defenses. Such cooperation would call for improved communication with governmental organizations, improving the speed and transparency of regulation development and industry support. When both sectors work together to share valuable data, they can ensure a quicker, more coordinated response to fraud incidents, ultimately reducing the financial impact and boosting consumer confidence. For example, well-shared data could enable the creation of an early-warning system, similar to initiatives in the UK, Philippines, Singapore, and Australia, helping to prevent fraud before it escalates.

Although bodies like the European Union take steps to prevent fraud and protect their citizens through regulations like the Payment Services Directive 3 ("PSD3") or Payment Services Regulation ("PSR"), there is still a significant gap in collaboration between FS firms and telecoms. At the outset, there is no need to create a new technical advanced solution, the core of solving the problem lies in joint collaboration, sharing data when needed.

Supporting industry efforts

At PwC we support our clients to stay on top of fraud risk management and cooperate with market leaders in the technology space. We are ready to help you uplift or design your fraud operating model and integrate the most suitable technological solutions that match your needs.

In conjunction with our technology partner Feedzai, we offer financial firms cutting-edge fraud management solutions tailored to address the specific risks of each organisation, whilst ensuring the highest level of system precision. Feedzai's solutions can utilise the data from telecoms and allow the FI to consume and combine them with other risk signals, which alongside machine learning models will uplift fraud detection capabilities. Feedzai's fraud capabilities combined with PwC's industry experience have elevated the fraud detection landscape in multiple banking projects.

If you are interested in learning more about industry leading practices or want to ensure you are aligned with current regulations, do not hesitate to contact our team.

Contacts

Vilém Dědek

Fraud Subject Matter Expert
PwC CEE Financial Crime

vilem.dedek@pwc.com

Tejal Kaur

Fraud & Identity Subject
Matter Expert, Feedzai

tejal.kaur@feedzai.com

Jeny Rasheva

Fraud Services Lead
PwC CEE Financial Crime

jeny.r.rasheva@pwc.com

Dan Holmes

Director of Fraud & Identity
Market Strategy, Feedzai

daniel.holmes@feedzai.com