Anita LeMaire, FIS

Anita LeMaire is the managing director of FIS in Australia and has been with the company for over 20 years. Anita manages the Banking and Payments Product Development team at FIS, which supports the company's international markets to deliver industry-leading solutions for clients.

Banks and fraud prevention in the COVID-19 era

Anita LeMaire

With Australia's COVID-19 vaccine program in full swing, businesses and banking institutions across the country are cautiously optimistic that the nation's economic recovery is about to kick into gear.

After taking a battering in 2020, the economy has been showing signs of a modest bounce-back, with GDP gaining 3.3% last quarter, as reported by the Australian Bureau of Statistics (ABS) in its 'Australian national accounts: national income, expenditure and product' release of December 2020. While these are promising signs that things are looking up, there are—as always—two sides to every coin, and with increased online spending comes greater risk of falling prey to fraudulent activity online.

If anything, 2020 was generous in its lessons. One of the most pertinent lessons was that fraud thrives in times of economic uncertainty. Thousands of Australians learnt this the hard way, with the Australian Competition and Consumer Commission's (ACCC) Scamwatch recording over 6,120 COVID-19-related scam incidents and more than $8,400,000 in losses since the pandemic first hit the country.

What is most interesting here is not the number of fraud incidents, but the nature of these attempts. The ACCC reported that $36,368,687 was lost in buying and selling, and that the vast majority of these taking place via email (over $20 million) and internet mobile applications (around $4.7 million).

With even the most vigilant consumers falling prey to these increasingly sophisticated fraud attempts, banking institutions are under more pressure than ever to equip their customers and employees with the knowledge and tools needed to avoid these threats entirely.

Educating from the inside out

When it comes to tackling new methods of fraud, knowledge absolutely is power. All functions and departments within the banking ecosystem can help minimise fraud. Whether it is the sales and marketing team ensuring the right information is reaching the customer at the right time, or cybersecurity analysts who must develop and analyse online behaviour models to detect fraudulent behaviours—each has an important role to play.

It is part of the banks' client service role to ensure they are providing the right information and resources to their customers to prevent them from being defrauded by bad actors online. Banking institutions can implement a variety of methods and tap into new channels to educate their customers about fraud detection and prevention, from online seminars, in-branch sessions, marketing campaigns and large-scale public education campaigns.

Education campaigns also play a key role in helping customers understand their own responsibilities when it comes to minimising the chances of fraud online.

When informing customers, banks should ensure they are highlighting clear, actionable steps customers can take, such as:

- having strong and secure passwords,

- deleting spam and suspicious-looking emails
- ignoring requests that ask them to call unknown or unverified phone numbers.

Contactless commerce a breeding ground for fraud

In Australia, the impact of social distancing orders on payment preferences were bifold. First, the nation immediately moved almost exclusively to non-cash transactions, to limit virus transmission through unnecessary cash handling. The impact was immense, with FIS' *The Global Payment Report 2021* finding cash payments accounted for just 8.3% of in-store transactions last year. The downward trend is expected to continue well after the crisis abates, with in-store cash transactions forecast to decline to just 2.1% by 2024.

Second, the ABS' 'Online sales, October 2020 – supplementary COVID-19 analysis' found that the ABS' 'Online sales, October 2020 – supplementary COVID-19 analysis' found that shopping reached peak highs with total online sales averaging an annual rise of 67.1% from March to October 2020. With fewer cash transactions taking place, fraudsters have been forced to seek out new avenues and channels to exploit.

From our research, we know people are increasingly using their mobile phones to purchase goods online, with mobile payments projected to account for 31% of all online transactions in 2024 compared to 24% in 2020. As a result, we have seen increasingly sophisticated attempts at mobile phone scams, in addition to phishing attempts, identity theft and fake email/ text messages.

While no-one is immune to these attempts, unfortunately it is often the most vulnerable groups in society—including older Australians, the young and people living with disabilities—who are disproportionately affected. At a time in which there is heightened anxiety around finances due to unemployment and lower-than-normal job security, it is integral that banking institutions are investing in the right resources and tools to combat fraud in order to protect their customers, particularly those most at risk.

Keeping guard

Institutions must now go above and beyond their previous call of duty and deploy the appropriate monitoring capabilities to protect their customers against fraud. This is especially true as consumers move away from cash-based transactions, and alternative payment methods gain traction.

With advances in technology creating new methods of payment such as QR code-based transactions and instant payments, there is a real need to adopt cross-channel monitoring to ensure customers are as protected as possible. This equals an omni-channel view of all transactions made, whatever the method of payment.

Institutions must have in place robust mechanisms to monitor account activity for unusual actions that either do not fit the normal behaviour profile of the consumer or breach the criteria of a rule defined in a fraud-monitoring solution. This is especially true for payments that are out outside on an individual's usual behavioural pattern, such as making payments to overseas or known fraudulent accounts.

Conclusion

The pandemic has highlighted the propensity for fraudulent behaviour to thrive in times of chaos and disruption. The past year is a testament to the fact that fraudsters will cash in on the confusion caused by social upheavals, including changes to how we spend and work. What we are seeing is a shift in tactics by organised crime as the opportunities on more traditional methods of payment fraud have been drastically reduced.

While it may be hard to conceive that there are people out there making a business out of exploiting vulnerable consumers, online fraud attempts are unfortunately one of the harsh realities of living in a digital world. The good news is, if banking institutions and their customers work together to stay up to date with the latest tools and resources, not only will they stay on top of emerging threats, but also remain one step ahead of fraudsters. **FS**

The quote

It is part of the banks' client service role to ensure they are providing the right information and resources to their customers to prevent them from being defrauded by bad actors online.