5 banking and payment security threats and trends to watch in 2023

By Gerhard Oosthuizen

27 Jan 2023

The digital pendulum is swinging back to pre-pandemic agendas, offering security leaders in the banking world a chance to revisit longer-term projects and take advantage of the tech crunch layoffs to bolster their security teams. This will be especially important as cyber criminals are also beginning to feel the pinch and are likely to increase their efforts.

Gerhard Oosthuizen, chief technology officer at Entersekt

People were so bullish about the digital spend in the Covid years that the retraction hitting large parts of the tech industry will take some by surprise – banks and credit unions included. Many of the important, but often delayed-due-to-Covid priorities will be put back on the 2023 to-do lists and we may also see many of the 'technical debt' and longer-term projects that were pushed out during the crisis, get their rightful place on this year's agenda.

In my view, it will be a year where we're going to see lots of different movements and initiatives get attention, as the 'digitise everything' focus that highlighted the past few years begins to wane.

However, as we continue through our crypto winter and tech crunch, security leaders should make use of the opportunity to snap up available skills. Because the one thing we know is that when things get harder, criminals also become more desperate. We must prepare for more breaches as the year progresses.

Here are five trends that will impact tech and security leaders in 2023.

- **Generative AI is all the rage, but it comes with a warning label:** If you haven't played with the newer AI chat and art generators, then you must at least have heard of them. The maturation of natural language text generators like ChatGPT and image generators like Dall-E 2, are testing our limits when it comes to differentiating between machine and human outputs.

These advancements offer organisations a huge opportunity when it comes to deploying chat technology as part of their self-service and broader omni-channel communication efforts.

Having a bot that is better able to interpret and easily respond to queries will put customers at ease and could rapidly improve automation efforts. This should attract particular interest from banks and other financial institutions and is likely to add some momentum to chat banking initiatives.

Should companies invest in ChatGPT?

18 Jan 2023

But as attractive as the additional automation may seem, security leaders will also need to gear up to deal with the darker side of the technology – or rather of the humans who use it for their nefarious ends.

One example is that some AI programmes can generate basic programmes which could help bad actors write code to bypass poorly secured websites. Another is that it is feasible to use these machines to simulate a voice (with just a small sample), which could then be used to bypass voice recognition or in payer manipulation fraud.

And, of course, the art generators are ideally positioned to help generate synthetic IDs with face images, voices and back-stories that don't actually exist, but look incredibly real. Fraudsters could even get advice on how to break security systems by just asking these AI systems to make recommendations.

While it's clear this technology has tremendous potential to improve the customer experience, it also offers fraudsters a host of new opportunities. Expect significant strides to be made on both sides during the year ahead.

- **Social engineering (especially payer manipulation) fraud will see a big spike:** There is no limit to human ingenuity, and payer manipulation (or authorised push payment) fraud is already being highlighted as a big area of concern. In fact, the UK has seen a 41% rise in authorised push payment in 2021 according to the UK's annual fraud report.

This type of fraud often has a fraudster calling a customer and convincing them they are about to have their money stolen, fast-talking them into transferring their cash into a mule account controlled by the criminal ring. Using the customer as the 'insider' that helps steal money has now been established as the most effective way to access funds.

Expect lots of new schemes emerging that will try to exploit this, and lots of marketing campaigns to educate and warn customers. We also expect a good deal more new technology firms emerging in this space with new innovation to prevent this kind of attack.

- **Increased regulations will add to the pressure:** Regulators will continue their efforts to protect the consumer (often from themselves) and businesses should prepare for added regulatory requirements in the coming months.

Widely regarded as a success in protecting customers, Payment Services Directive Two (PSD2) will be extended with PSD3 in the EU in 2024. It's expected that more focus will be placed on improving user experience and, wherever possible, removing them from the authentication process in order to reduce friction.

Dion Chang: #BizTrends2023: How the rise of the machines will impact 2023

27 Jan 2023

In addition, Europe has published their eIDAS 2 regulations requiring governments to start issuing digital identities, with the first pilot kicking off in March 2023. This will be driving digital identity in the region over the coming years.

Overall, we're also seeing a lot more organisations, such as EMVCo, Visa, Mastercard and The National Institute of Standards and Technology (Nist), increase their security requirements and include Fido authentication into their standards and regulations.

With this regulatory backing and support from Apple, Google and Microsoft, Fido authentication will receive a lot of attention. The US government, meanwhile, has committed to Zero Trust architecture and has placed significant emphasis on stronger enterprise identity and access controls, including multi-factor authentication (MFA).

Many vendors are jumping on the bandwagon and security leaders will be hearing a good deal more about this during the year.

- **Digital ID hits its stride:** With the regulatory support behind it, and eIDAS 2 coming into effect in 2024, we expect to see digital ID building on the small strides made in 2022, with Estonia and Canada already having built out various systems.

The US has also dabbled with it in a few states and Apple is co-ordinating with travel agents to load drivers licences as part of its wallet offering.

R25m facility gears up to shake up the banking industry through novel distribution model

Katja Hamilton 5 Dec 2022

With the first pilot in the EU underway, many private and public organisations will likely begin factoring digital ID into their thinking.

The European approach is based on emerging standards from the self sovereign world such as the W3C's verifiable credentials, while Apple has chosen NFC standards from the ISO. It will be really interesting to see if these two diverging standards will find a way to work interoperably, or if one will dominate.

- **Passwordless thinking will continue to gain momentum:** We identified the rise of a passwordless future in previous predictions and we still hold that this will be a big trend on the radars of chief technology officers and chief information security officers this year. The renewed commitment to Fido will aid the move towards a passwordless world and security leaders can confidently move forward with their plans to slash the friction in their user experience.

Finally, we know that predictions can be foolhardy in a world as mercurial as the one in which we find ourselves. However, when we asked ChatGPT what its top five predictions for digital fraud in 2023 were, its number one concern was ironic, but perhaps indicative of just how 'self-aware' AI is becoming. It's answer? "Increased use of deepfake technology to create convincing impersonations of real individuals for fraudulent purposes."

And so, I remain confident of my 2023 list.

ABOUT THE AUTHOR

Gerhard Oosthuizen is the chief technology officer at Entersekt.