SYNECTICS SOLUTIONS

FROM REVOLUTION TO EVOLUTION: WHY FINANCIAL INSTITUTIONS MUST ADAPT TODAY FOR A SECURE TOMORROW

For businesses, adaptation has always been key to survival. And in no industry is embracing change more vital than the financial industry. In our ever-evolving technological era, it's necessary to remain relevant or risk becoming quickly outdated. History tells us that those who endure are those who adapt; those left standing are those who keep up with change. But how are traditional institutions adapting to digitisation? And what barriers are challenger banks facing with data management and fraud prevention?

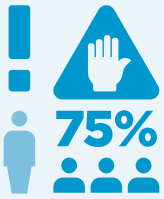
Both small and large organisations need to implement new technological innovations to ensure they have a secure tomorrow. Fail to keep up and financial institutions will become easy targets for cybercrime or fraud and hard-earned reputations will be ruined.

"Some organisations are reaping the rewards of the protective power of technology. But due to cost implications or restrictive, ancient systems, others fail to benefit from technological innovations."

Embracing change and maintaining trust

Attracting and maintaining customers is all about trust. Your customers need to feel secure. If your customers lose faith in you, they will quickly go elsewhere. A recent study by FireEye revealed that a whopping 75% of 1,000 UK respondents would lose all trust in an organisation – and would no longer use their services – in the event of a cyberattack. So safeguarding against threats of this kind has never been more important for your organisation. It has never been more vital to utilise technological innovations to help to improve your ability to detect and prevent fraud.

75% of 1,000 UK respondents would lose all trust in an organisation – and would no longer use their services – in the event of a cyberattack.



Historically, customers have been hesitant to switch banks. But this would appear to be changing. Perhaps the reluctance to change is the mindset of an older generation. Our digital natives, and the vast majority of our fully converted digital migrants, would certainly have less reluctance. An increasingly tech-savvy consumer base demands convenience, real-time solutions and new digital products and services.

But dealing with a paradigm shift of such magnitude, not seen before in hundreds of years of banking, is resulting in many financial institutions being slow to react or struggling to adapt.

The rise of the machine

The financial industry has come a long way from the beginning of its technological revolution back in 1967, when the world's first ATM was installed in London by Barclays Bank. This revelation of convenience was a game changer. And over the last 50 years, customers have continued to demand even more convenience.

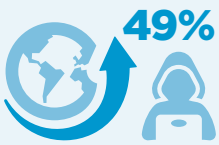
But as banks switch more services to digital to satisfy the demands of its customers, they broaden their exposure to attack. Digital services are what customers demand, but this also makes financial institutions a larger target for cybercrime and fraud.

The digital age has brought with it many benefits, but it has also caused many new concerns for the industry. And none more concerning than the cybercriminal and organised financial crime gangs.

The rise of cyber fraud

With the financial crisis of 2008 still fresh in the memory of many, 10 years on and financial organisations face very different dilemmas. Recent years have seen a surge in online fraud. Financial Fraud Action UK claims that remote banking fraud rose to a staggering £73.8 million last year. And according to PwC's 2018 Global Economic Crime and Fraud Survey, a whopping 49% of global organisations have experienced economic crime in the past two years. Fraud is fast becoming a growing issue for financial institutions, as tech-savvy criminals increasingly target the payments industry in new and inventive ways.

49% of global organisations have experienced economic crime in the past two years.



From deception and impersonation scams to sophisticated malware and data breach attacks, fraudsters have their sights on one thing: your customers' personal data. And once they have it, the consequences can be costly. So as cases of economic crime show no signs of slowing, it's important to realise the impact that fraud can have on your organisation. A cyber fraud attack will not only be massively disruptive and costly, but this type of infiltration will be seriously damaging to your reputation, will negatively impact employee morale and will harm business relations.

WannaCry, which shifted cybercrime to the forefront last year, confirmed that no institution is safe from this type of attack.

"...fraudsters have their sights on one thing: your customers' personal data. And once they have it, the consequences can be costly."

Sadly, financial institutions are like magnets to thieves. And it can be hard to keep up with the ever-changing landscape of fraud and financial crime, as criminal methods continually change and become more organised. Our latest statistics show that organised fraud rose to 59.58% during 2017, which is a clear increase on the 57% for the same period the year before.

Criminals constantly find new ways to perpetuate fraudulent activity, so it's important to update your data insights and your organisation's ability to detect and prevent fraud fast enough to fight this constant threat. Outdated defences won't keep you safe. To fight modern-day criminals, you need modern-day weapons. Some organisations are reaping the rewards of the protective power of technology. But due to cost implications or restrictive, ancient systems, others fail to benefit from technological innovations.

Our latest statistics show that **organised fraud rose to 59.58% during 2017,** which is a clear increase on the 57% for the same period the year before.

The situation with start-ups

As established high street banks wrestle with old business processes, new challenger and mobile banks are swooping in. These digital-first banks are emerging in reaction to the growing number of customers who would prefer to have their finances at their fingertips. By 2020 it's estimated that the number of people who use mobile banking apps is set to reach a staggering 2.3 billion. This new wave of start-up banks offer personalisation, 24/7 online access and real-time payment notifications, appealing to the growing demand for convenience and instantaneous action. The simplicity of this banking solution even extends to new accounts.

New customers can quickly, easily and instantly open an account online, without all the hassle of travelling into town, filling out endless forms and waiting days for approval. It would seem these tech-savvy start-ups have it all. So what's stopping them from harnessing technological innovations to help prevent data theft and fraud? Although these small-to-medium enterprises are more flexible and can much more easily integrate new systems, finding the funding to take on and train the right people to deal with the latest data science tools and techniques can be an issue. Expertise is costly.

These new institutions also often struggle with the small amount of customer data available to them, which makes it difficult to perform quality analysis to identify trends.

But without these insights many challenger banks risk falling foul of fraudsters.

"Open banking promises to make the industry more competitive, as customers take control of their own data and are no longer tied to the offers and rates of one particular bank. But will this new regulation also create greater opportunity for fraudsters?"

The trouble with the traditional

Established financial institutions face very different challenges. Although large establishments have years of historical data, organisational structures and company hierarchies can block innovation. For these firms, demolishing and redesigning legacy architecture has huge overheads. These massive company changes create significant costs, take serious time and demand specialist skills. Redesigning outdated, complex business processes across entire organisations is a slow and laborious undertaking.

But despite the enormity of the task these institutions are making massive changes to their processes and procedures. They are desperately trying to adapt to meet the demands of our ever-developing digital age. But until they fully evolve, they too risk falling foul of fraudsters.

Although they wrestle with different restrictions, both small-to-medium enterprises and larger institutions need to break down their barriers to technology. If they don't, they will fail to protect themselves and their customers. And may lose the battle completely.

"...they are desperately trying to adapt to meet the demands of our ever-developing digital age. But until they fully evolve, they too risk falling foul of fraudsters."

A secure tomorrow

The secure financial institution of tomorrow will be one that adopts the technological innovations of today. The organisations embracing technology through automation, predictive analytics and artificial intelligence are the ones that will benefit from valuable data insight and the improved ability to detect and prevent fraud.

By fighting back with the latest weaponry, these companies will make themselves a harder target.

With advances in AI and machine learning, you can help protect your institution, shareholders and customers from these relentless fraudsters. Cybercriminals, and those looking to perpetuate fraud or financial crime, are using increasingly clever techniques.

But thanks to technological innovations, you can stay one step ahead. Machine learning systems will increase your defence measures; these self-educating systems can learn, adapt and reveal any developing patterns that may suggest fraudulent activity. And the more data they accumulate, the more effective they become at detecting fraud and keeping your organisation safe. This technology will also reduce the amount of time your people waste investigating false positives.

The secure financial institution of tomorrow needs to invest in the right technology, the right people and to collaborate to increase the volume and variety of the data they capture.

The power of technology

Banks and financial institutions are beginning to realise the enormous potential of data. Not just to fight fraud, but to enhance the customer experience. These intelligent systems have the ability to offer your customers real-time services. They can assess borrowing patterns, evaluate risk and transfer funds in an instant. As Darryl West, Chief Information Officer at HSBC bank stated last year, "Apart from our $2.4 trillion dollars of assets..., we have at the core of the company a massive asset [in the form of] our data". Over the last few years HSBC has been reaping the rewards of machine learning and data analytics.

And these technological innovations are bound to become ever more vital, as we edge further into what has already been a radical year for the financial industry. January's implementation of the Second Payment Services Directive presents another massive shift for both banks and customers alike. Open banking promises to make the industry more competitive, as customers take control of their own data and are no longer tied to the offers and rates of one particular bank. But will this new regulation also create greater opportunity for fraudsters?

As account aggregation will now no doubt soar, it's likely that increasing numbers of customers will use personal banking apps to combine their finances, putting all their accounts in one place – and at the tips of their fingers. PwC predict that a huge 20% of all online transactions will be made through apps this year.

This surge in mobile banking will obviously demand even more technological investigations by financial institutions, in order to monitor the apps and keep them secure. All organisations will need to adopt the protective power of technology to fight the online fraudster.

This game-changing initiative is also likely to drastically increase the rates of bank account switching. So to keep your customers, it's imperative to keep your institution safe.

The secure institution of tomorrow will adopt the benefits of big data – understanding, predicting and improving. And will embrace change.

How Synectics Solutions can help you

At Synectics Solutions we welcome change and continually push boundaries. It's this innovative spirit that has positioned us as a leading software provider for the financial industry and why 98% of our clients establish long-term partnerships with us.

Supported by us and our data science capabilities, your institution will become safer and more intelligent. You will be able to make better decisions, reduce risk and become more efficient. As the late, great Stephen Hawking said, "Intelligence is the ability to adapt to change". We can help you adapt, with our value-driven fraud prevention software.

With SIRA, Orion and Precision, you will reduce losses and maintain customer trust. Our fraud prevention and detection solutions will help your organisation to evaluate large volumes of data, respond quickly to future trends, reduce false positives, fast track good customers and easily identify existing and emerging suspicious network activity.

By supporting your organisation with our fraud prevention and detection solutions, we can help you overcome potential threats, implement change and successfully adapt for a secure tomorrow.

For more information about Synectics Solutions call **01782 664000** or email **info@synectics-solutions.com**

Synectics Solutions Ltd, Synectics House, The Brampton, Newcastle-under-Lyme, Staffordshire, ST5 0QY

+44 (0) 1782 664000 | info@synectics-solutions.com | www. synectics-solutions.com