Some sectors make better targets for fraudsters than others

How can at-risk industries keep their customers safe?

Government agencies, healthcare and financial services have become attractive targets for bad actors, where a successful fraud hack can be highly lucrative, either as a result of stealing funds directly or stealing valuable customer data.

These organisations hold a whole load of highly confidential data—whether that's financial or other information— data that can subsequently be used elsewhere for a secondary fraud event, says Mike LaCorte, CEO of the investigations, security and intelligence agency Conflict International.

For many years, firms in highly regulated sectors have relied on outdated technology to protect customer data from unauthorised access. Often that has enabled fraudsters to stay one step ahead, according to **Chris Michael, co-founder and CEO of open finance platform Ozone API.**

52% of companies with $10 bn in revenue experienced fraud in the last 24 months

18% of companies faced $1m in financial repercussions as a result

Source: PwC's 2022 Global Economic Crime and Fraud survey

"Once a bad actor gets in, they get access to almost anything."

Organisations can spend millions on having the best firewalls and cyber defences, but negate the human element that contributes to fraud, one simple email or phone call can let a fraudster in. Fraudsters are always looking for vulnerabilities and loopholes they can take advantage of.

Chris Michael says "*companies need to devise new policies and build systems to ensure strong identity verification that validates devices and users prior to granting access".*

"You need to have a proper way of verifying that changes to payment instructions are right and ensuring who you're talking to is the right person—not everyone is who they appear to be,"

Knut Ronning, CFO at Xledger.

1. Go passwordless. Instead use a blend of cryptography, secure devices and biometric authentication to remove the need for customers to use passwords, thus reducing the risk of them being shared or stolen.
2. Use a tiered approach to customer risk profiling. Customers that pose a higher risk may be subject to more stringent controls, giving them a choice of control depending on their level of risk.
3. Train employees. They must be able to recognise tell-tale signs of fraud. Discrepancies in invoices or payment instructions or an unrecognised account should instigate a response from staff.
4. Be wary of third-party risk. If suppliers have gaps in their defences, fraudsters can exploit them and gain access to systems through the back door.

"You need to understand your suppliers' systems and controls in the same way that you would your own," says Peter Hucker, head of operations at Xledger. *"This is really about finding the weakest link, and if your supplier is the weakest link, then you have a problem. That often can be a place where businesses slip up."*

Data, analytics and technology solutions for business

Equifax customer verification solutions are a complementary collection of cloud-based tools that help you establish a genuine identity with a high degree of confidence, and meet industry and regulatory standards.

At Equifax we look beyond the direct evidence of fraud or misrepresentation to connect accounts, people and devices that might seem unrelated. Our Identity verification solutions help you spot suspicious behaviour or anomalies and prevent fraud from sources that otherwise appear genuine.

Anti-Money Laundering Verification

Equifax Commercial AML is a powerful business entity verification solution that supports Customer Due Diligence (CDD). Validating a firm plus its officers adds a deeper level of awareness to the Know Your Business (KYB) evidence gathering process that's required in line with regulations when establishing a business relationship.

Our Watchlist Check screens against worldwide sanctions, politically exposed persons (PEPs) and relative and close associate data to support compliance with AML regulation, it additionally provides special interest persons (SIPs) and special interest entities (SIEs) screening to highlight high level crime and the associated potential risks.

We help reduce uncertainty or compromise across your identity and AML processes, so you can say "yes" with more confidence. Talk to us today about adding an extra layer of protection to your customer identity verification journey.

For more information please visit equifax.co.uk or contact your account manager