Article

De-risking highly regulated industries

Some sectors make better targets for fraud than others. How are the most at-risk industries keeping their customers safe—and happy?

> “So not only are these regulated institutions subject to fraud, it’s not just the asset that’s at risk, it could be data that can subsequently be used elsewhere for a secondary fraud event.”
>
> **Mike LaCorte**

Putting a price on identity is not something that most of us have given much thought. Even still, the black market for sensitive personal information is flourishing. From bank login credentials to complete medical records, almost nothing is off limits to artful and ambitious cybercriminals operating on the Dark Web.

As businesses and their customers increasingly depend on digital platforms to set up accounts and secure transactions, protecting those online spaces needs to be a priority. And while this rationale applies across sectors, nowhere is it more crucial than in highly-regulated industries.

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

Mike LaCorte, CEO of the investigations, security and intelligence agency Conflict International, explains: “As well as assets, they hold a whole load of highly confidential data—whether that’s financial or other information—that cybercriminals can use to their advantage, especially in a layered fraud type scenario.

"So not only are these regulated institutions subject to fraud, it's not just the asset that's at risk, it could be data that can subsequently be used elsewhere for a secondary fraud event," he continues.

For many years, firms in highly regulated sectors have relied on outdated technology to protect customer data from unauthorised access.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.

"Many of these technologies were based on the concept of a hard shell—firewalls and strong passwords—but with a soft centre containing large honeypots of data, all in one place and often not encrypted in transit or at rest," says Michael. *"Once a bad actor gets in, they get access to almost anything."*

But even with top-of-the-line tech, cybercriminals often focus their attacks on individuals who may lack sufficient fraud awareness and can easily be duped into clicking on a malicious link.

"There's a whole human element side of fraud that is sometimes overlooked," says LaCorte. *"You could spend millions in having the best firewalls and cyber defences, and then just a simple email or phone call can let them in. Fraudsters are always looking for vulnerabilities and loopholes they can take advantage of."*

More than half of businesses with $10 billion or more in annual revenue said they had experienced fraud in the past 24 months, according to PwC's 2022 Global Economic Crime and Fraud survey. All of this, combined with a rise in fraud more generally, means that firms must take a dual approach to risk management that incorporates both technology and training.

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

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

PwC, 2022

“It’s about what is proportionate in order to preserve the customer experience but keep the integrity and the compliance of the organisation that is holding the data, but it is a balancing act. There isn’t a simple answer as to where to draw that line.”

Mike LaCorte

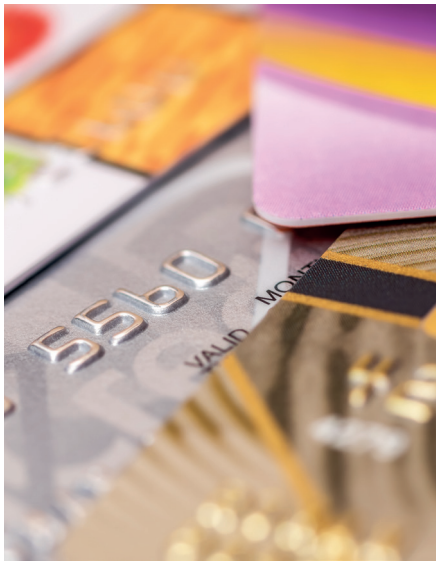
A number of firms have already started to implement much better tech to protect their data, says Michael. For instance, more firms are adopting concepts such as ‘zero trust’—a set of principles that effectively discourage firms from implicitly trusting networks or devices used to access and store data.

Instead, companies need to devise new policies and build systems to ensure strong identity verification that validates devices and users prior to granting access, he says.

Some are also seeking to go passwordless and instead use a blend of cryptography, secure devices and biometric authentication to remove the need for customers to use passwords, given how easily they can be shared or stolen.

When it comes to training, employees must be able to recognise tell-tale signs of fraud. Discrepancies in invoices or new payment instructions that involve sending money to an unrecognised account should immediately sound alarm bells, says Knut Ronning, CFO at Xledger.

"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," says Ronning. Organisations also need to be warier 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 that businesses slip up."*



Some firms are taking a tiered approach to customer risk profiling, where customers that pose a higher risk may be subject to more stringent controls.

"We give customers a choice of controls depending on their level of risk," says Hucker. *"So we might demand more of users of our finance system. To some extent, we let our customers decide on their level of controls, providing it doesn't fall below our overall security measures."*

This underscores the challenge many regulated firms face when reconciling risk management and compliance controls with successful customer experience.

"It's about what is proportionate in order to preserve the customer experience but keep the integrity and the compliance of the organisation that is holding the data," says LaCorte.

"But it is a balancing act. There isn't a simple answer as to where to draw that line."

We help reduce uncertainty or compromise across your identity 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