|  |
| --- |
| FrontPageBackgroundImage |

**Publication date:**   
22 Mar 2024   
**Author(s):**   
Ouliana Smith, Senior Research Analyst, Financial Services

# DT Fraud Conference: Why standards are important to mitigate evolving threats in payments

## Omdia view

### Summary

On March 6 and 7, 2024, payments professionals gathered at the annual DT Fraud Conference taking place at the Leonardo City Hotel, London, to hear a range of presentations from companies, technologists, and regulators in the space. Across all the sessions the prevailing trend was the proliferation of risks faced by the sector. In this summary we unpack the key themes and the importance of standards.

### Standards to address the scale and seriousness of new risks being created

Paul Lucraft of DT Fraud Conference and Expense Reduction Analysts kicked off the event, having the hard job of summarizing all the themes, innovations, and challenges at the intersection of payments and fraud in just half an hour. In his presentation he underscored how far ahead criminals are and, consequently, how much work the sector has to do to deliver everything that consumers expect.

Commenting on the event, Lucraft stated:

*Fraud and risk management is core to the commercial models that drive banking and payments ecosystems. Incentivizing best practices, encouraging innovation and aligning with appropriate regulation, compensating innocent users, and ensuring that there are guarantees around payment methods are all contributors to how that complex interconnected web works.*

*Through this year’s conference we dissected some of the sector’s challenges and explored the areas where we see change and where businesses will be able to optimize secure payments in coming years.*

In one sense the absolute number of risks the sector is facing is increasing. As the number of new payments technologies grows, not only does it create more individual risks, but the number of cracks between different systems multiplies the potential exploits. Second, there is evidence that criminal actors are increasingly agile and, more importantly, networked. Criminals have always enjoyed the fact that they are able to act faster and with fewer limitations than their adversaries, but this trend is accelerating. Rather than limiting themselves to one or a few types of fraud, criminals are increasingly able to use the same types of innovation as the legal payments industry, leveraging automation and artificial intelligence (AI) strategies to accelerate their activities to new levels of intensity.

The increasingly networked elements of fraud involve the recognition that instead of thinking solely about second- and third-party information risk, the criminality of the dark web creates fourth, fifth, sixth, and onward risk profiles. Illegal data brokerage and the solidification of a “fraud for hire” industry has opened up payments fraud to a larger number of criminals and makes mitigation much harder.

In our recent client reports and thought pieces, Omdia has already noted the potential for such organized and flexible criminality. As open banking increasingly looks to require a form of digital identity to leverage all the data needed, it has the effect of concentrating a very large amount of information into a single technology center.

The worrying counterpoint to this is that, looking at most organizational ontologies across financial services, each part of the fraud process from detection all the way through to eventual redress tends to be in a siloed department: an agile, networked approach to the issue is not in evidence across the payments industry as a whole as it is in the criminal space.

Omdia has provided commentary on the importance of standards and technical interoperability to help deliver the promise of so much in the payments industry; now there are a lot of different products and innovations that are developing on different trajectories, and the line between a “tech” industry and a “banking” industry is increasingly arbitrary. It is far from clear which tools, products, or technologies will become dominant over the next five years.

Therefore, I thought the session on evolving standards by Charles Brookson of Azenby and Zeata Security, in communications networks and regulatory expectations, was easily the most consequential. The only long-term way of addressing all of those risks around the number of gaps between different technologies and products and reducing the options available to criminals is to work to a set of high and overarching standards. The ambition is to create a tide that lifts all boats in the payments sector. Developing high-quality technical standards is not just about trying to anticipate and mitigate risks in the sector; it is also about accelerating and amplifying the pace of innovation to build as well as secure.

If the payments technology space is underpinned by robust quality standards then innovators know what they are working with and can develop products and tools that they know will deliver what that market needs.

Omdia has reported on the damage that uncertainty causes fintechs: uncertainty in terms of long-term regulatory visibility and uncertainty of regulatory dissonance between jurisdictions as a result. Standards are important at a technical level, but they are arguably more important at a strategic level: they are the main means by which a lot of the uncertainty in payments innovation can be taken away, and the gap between proof of concept and sustainable commercial traction can be reduced.

In all, the conference provoked a surprisingly emotional response: payments is such a vibrant sector that is currently innovating at an almost impossible pace, but at the same time, the speakers crystalized the scale and seriousness of new risks being created.

## Appendix

### Further reading

[*Market Landscape: Open Banking*](https://omdia.tech.informa.com/om120539/market-landscape-open-banking)(March 2024)

[*Market Fundamentals: A Trajectory of Open Banking*](https://omdia.tech.informa.com/om120898/market-fundamentals-a-trajectory-of-open-banking)(March 2024)

### Author

Ouliana Smith, Senior Research Analyst, Financial Services

[askananalyst@omdia.com](mailto:askananalyst@omdia.com)

### Citation policy

Request external citation and usage of Omdia research and data via [citations@omdia.com](mailto:citations@omdia.com).

### Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia’s consulting team may be able to help you. For more information about Omdia’s consulting capabilities, please contact us directly at [consulting@omdia.com](mailto:consulting@omdia.com).

### Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the “Omdia Materials”) are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together “Informa Tech”) or its third party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

### CONTACT US

[omdia.com](https://omdia.tech.informa.com)

[askananalyst@omdia.com](mailto:askananalyst@omdia.com)