SECURING FINANCIAL SERVICES

July 2nd, 2025, London, UK

Securing the Future of Finance

Hyper-personalized AI-driven banking, banking-as-a-service, DeFi, crypto – can security cope with innovation?

https://akjassociates.com/event/finserv

AKJ Associates

Balancing innovation, compliance and security

The rise of AI-driven hyper-personalization, platform banking, super-apps, Banking-as-a-Service (BaaS), and DeFi/crypto presents a range of cybersecurity challenges and regulatory concerns.

The AI models that drive personalization (and those in fraud detection and credit scoring) can be attacked via Adversarial AI, Model poisoning and Bias exploitation.

Super-apps & platform banking integrate multiple financial services, third-party partners, and open APIs. This creates issues both with integration of legacy systems but also an expanded attack surface with more entry points for hackers due to interconnected services.

Cloud and de-centralized banking models, such as super-apps or platform banking initiatives, increase these risks and add others. Cloud-first banking and open APIs increase misconfiguration risks. Third-party integrations may expose sensitive data. And insecure API authentication is a hard-to-detect and dangerous threat vector.

Embedded finance & BaaS allow non-banks to offer banking services, introducing new players into the ecosystem who may not be as well defended as highly-regulated banks, insurers and asset managers. And then DeFi & crypto operate with pseudo-anonymous transactions increasing the risk of fraud, money laundering, and synthetic identity theft.

DeFi and crypto does not just mean the wilder ends of the digital asset spectrum either: central bank digital currencies and the tokenisation of traditional financial assets are developing fast, and introduce huge additional cybersecurity challenges and risks.

And that is without even starting to think about the threats posed by Quantum Computing and the threats to traditional cryptographic algorithms, compromising banking security.

All of this has spurred a huge burst of regulation. In open banking & API security we have the EU's PSD2 & PSD3, the UK's Open Banking Standard and the US CFPB's 1033 Rule. Around Cloud and platform banking compliance we have DORA, the US FFIEC cloud computing risk guidelines, and the UK FCA's operational resilience framework (PS21/3).

AI & ML in banking is now a big focus (as is the data quality these models will rely on). So, we have the EU AI Act. We have US Regulators the OCC, CFPB, and SEC all expecting AI models to follow explainability and fairness standards. And the Basel Committee on Banking Supervision (BCBS) has issued guidance on AI/ML governance frameworks.

For DeFi, Crypto and digital assets the EU has MiCA to address AML, fraud risks, stablecoins; in the US SEC and CFTC have been increasing oversight of crypto markets and DeFi, at least until recently. And FATF has recommendations on KYC, AML rules for crypto and DeFi platforms.

So how can banks balance all of this innovation with security? This event will look at, amongst other topics, how banks are:

- **Strengthening AI/ML governance to prevent fraud & bias exploitation.**
- **Securing APIs & cloud services to prevent platform banking breaches.**
- **Ensuring digital identity security in DeFi, BaaS & embedded finance.**
- **Preparing for quantum-resistant security before threats materialize.**
- **Ensuring compliance with all of the new regulations without stifling the business**

Securing Financial Services will look at how leading institutions are continuing to develop their security and resilience programmes.
Join our real-life case studies and in-depth technical sessions from the security and privacy teams at the UK and Europe's most sophisticated firms.

Securing Financial Services

SECURING
FINANCIAL SERVICES

Key Themes

Securing AI-driven hyper-personalization

Banks need to implement AI model security frameworks (adversarial AI detection, bias correction). They need to use explainable AI (XAI) to audit decisions and detect model anomalies. And they need to deploy AI fraud detection on top of AI-driven banking (double-layer security) **Can you help them with these new challenges?**

Securing DeFi and digital coins

DeFi is a financial ecosystem built on public blockchains (like Ethereum) that provides financial services without intermediaries such as banks. But there are still linkages with 'TradFi', including banks' own DeFi efforts**. So what are the cybersecurity implications for banks and where do they need to look at strengthening controls?**

Securing Cloud-first and BaaS banking models

Banks need to move to hardened versions of Zero Trust and to next generation API Security to secure the open APIs new models require. So how do they guarantee robust authentication and monitoring that can dela with modern API-driven and cloud-based attacks? **Can you provide solutions or architectures to help?**

Securing tokenisation

Tokenization bridges traditional finance (TradFi) with blockchain, creating digital versions of real-world financial assets. And it's gathering pace. The security implications are then around blockchain, smart contracts, attacks on tokenisation platforms, attacks on custody and wallet infrastructure and 'oracle' corruption risks. **Can you help?**

Securing Open Banking and ecosystem models

Legacy systems problems, the same API issues as occur with super-apps and BaaS, and the additional third-party risks created by Fintech and non-bank integrations create vulnerabilities in innovative banking models. **So, what are the next gen IAM, real-time API security and other security solutions required to keep these new models safe?**

Securing the Quantum world

Banks need to prepare for quantum now. Starting with a cryptographic audit to identify weak points and the adoption of NIST-approved post-quantum cryptography (PQC). They also need to work with vendors to ensure quantum-safe compliance and to plan for "harvest now, decrypt later" attacks. **How can you work with the industry to keep it quantum-safe?**

We deliver your message direct to decision-makers

SECURING FINANCIAL SERVICES

Plenary Speakers

The e-Crime Congress Series events offer sponsors the opportunity to deliver content in a number of different ways.

Plenary speakers **deliver their presentations on the day of the event from a fully featured AV stage to a face-to-face audience**.

Their presentations can contain slides, video and audio and speakers can deliver their speeches from the podium or from any point on the stage.

Plenary presentations are 20 minutes long and take place in the main event auditorium guaranteeing access to the largest possible audience of cybersecurity professionals on the day.

Presentations are generally designed to be informative, topical and actionable, with the use of case studies and up-to-the-minute references to current developments.

Double-handed talks with clients are also welcomed.

Education Seminars

At pre-defined points in the day, attendees will be notified that the main plenary sessions are making way for a series of in-depth technical break-outs.

These sessions of up to 30 attendees are held in break-out rooms and delivered live to attendees.

They are an opportunity for vendors to deep-dive into a topical problem, technology or solution in front of a group of cybersecurity professionals who have self-selected as being interested in the topic being discussed.

They are also the ideal venue for solution providers to go into technical detail about their own products and services.

These Seminars run simultaneously, and attendees choose which session to attend.

At the end of the Seminar, attendees are notified that Networking time is now available before the next Plenary session.

Your team and your resources available in real-time

Exhibition Booths

Sponsor packages that contain an Exhibition Booth give sponsors the opportunity to be present in the main networking area of the event.

At these booths, sponsor representatives can interact with delegates face-to-face, deliver messaging and technical information via video presentations, demo products using their own BYOD technology and to distribute printed marketing and product information.

Sponsors may wish to consider different ways to drive footfall to their booths.

For example, sponsors who have presented in Plenary or in an Education Seminar can close their presentations by directing the audience to their booths.

And there are additional gamification elements available, including sponsor-supplied prizes, that can effectively drive traffic to booths.

We deliver the most senior cybersecurity solution buyers

SECURING FINANCIAL SERVICES

Our USP? We put buyers and sellers together

We understand that every vendor needs to sell more. That is the bottom line. This is even more necessary in the present situation.

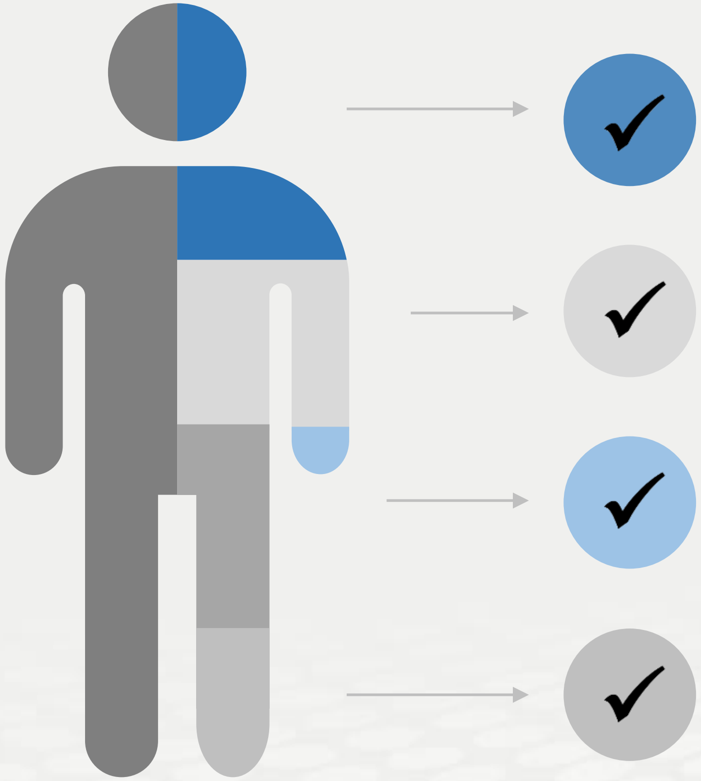
You will have access to the most senior buying audience in the cyber-security market.

AKJ Associates has been building relationships with senior information risk and security professionals for 20 years and our cybersecurity community is the largest of its kind globally.

We know the senior executives who drive strategy from the top, we know the enterprise architects who often control the largest budgets and we know the IT Security Leads and Engineers who so often dictate the purchase process.

All of these job titles attend e-Crime & Cybersecurity Congress events.

Getting access to the right people at the right time always increases the lead generation and always increases profitable sales activity.



Cyber-security

We have a 20-year track record of producing the events cyber-security professionals take seriously

Risk Management

We attract senior risk officers with responsibility for information risk assessment and mitigation

Fraud, Audit, Compliance

We provide the go-to events for fraud prevention and compliance owners at the world's key corporates

Data Protection & privacy

We are a key venue for decision-makers with budget and purchasing authority

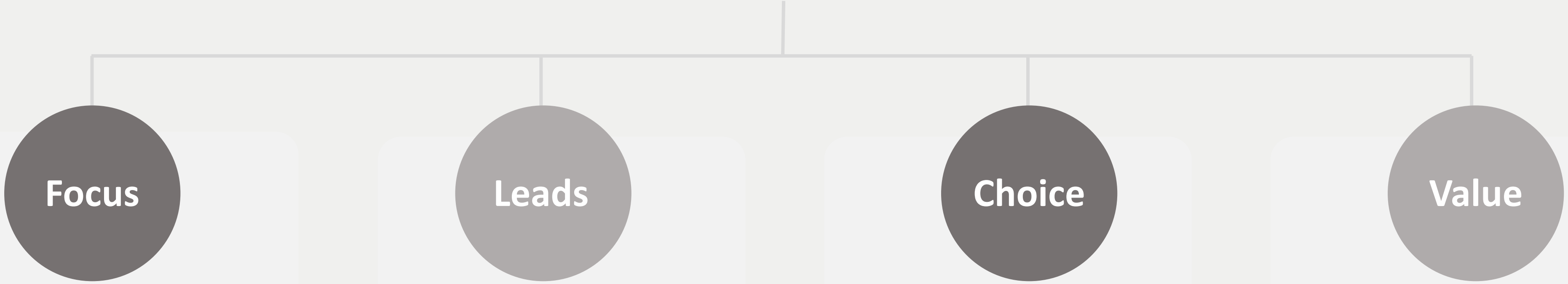
We deliver the most focused selling opportunity

SECURING FINANCIAL SERVICES

Specific, actionable and relevant information for time-constrained industry professionals

SECURING FINANCIAL SERVICES

The perfect platform for solution providers to deliver tailored advice to the right audience



Target growth

Each event represents a targeted opportunity to address the needs of a specific community whose need for your solutions and services is growing.

Boost sales

Sponsors can tailor messages to the needs of an audience that shares similar concerns and challenges, looking for solutions now.

Meet commercial aims

We work with sponsors to ensure they meet their commercial aims. We offer a number of sponsorship options, each providing specific benefits.

Showcase solutions

Our events provide sponsors with a unique platform to showcase solutions, as well as provide advice on how best to solve delegates' key challenges.

Securing Financial Services

SECURING FINANCIAL SERVICES

Delegate Acquisition

- The e-Crime & Cybersecurity Congress has the **largest community of genuine cybersecurity stakeholders** to invite to our events.
- Our reputation for hosting **exceptional events with informative content, excellent networking opportunities and the best vendor partners** means delegates know they are attending a quality event, and are willing to give up the time to attend.
- Our delegates are **invited by an in-house delegate liaison team** who call senior security and privacy professionals at public and private sector companies with a personal invitation to attend
- We **follow up all registrations** with further calls, emails on logistics requirements and reminders to **ensure the best possible attendance**.

Lead Sourcing

- The e-Crime & Cybersecurity Congress prides itself on **putting the key cybersecurity buyers and sellers together**
- To offer you the best prospects to network with, **we don't invite academics, job seekers, consultants,** non-sponsoring vendors or marketing service providers to this closed-door event. This **attention to quality over quantity** has been the hallmark of AKJ's events for 20 years.
- Each of our vendor partners will receive a delegate list at the end of the event.
- Through our targeted networking breaks built into our agendas you will have **unrivalled opportunities to network** with high-quality prospects with face-to-face networking at the event.

Get Your Message Across

- **Content is king,** which is why the e-Crime & Cybersecurity Congress prides itself on delivering informative and useful content, to attract senior audiences of decision-makers.
- Deliver an exclusive 20-min keynote presentation in the virtual plenary theatre, or host a 30-min targeted workshop session: good content drives leads to your booth, and showcases your company's expertise
- AKJ's in-house content / research team will complement the agenda with best practice from leading experts and senior security professionals from the end-user community
- If you are not presenting, the exhibitor booth offers the opportunity to share white papers and other resources for delegates to takeaway

Exclusivity Delivered

- AKJ Associates has never done trade shows. We see most value in working with **a select number of the top vendor partners**, and offering those companies the best access to leads.
- Our events keep the same ethos as when we first started 20 years ago, limiting vendor numbers. We will not be a hangar with hundreds of vendors competing for attention. We will keep our **events exclusive to give the best networking opportunities**.
- All booths offer the same opportunities with the same capacity and functionality regardless of the vendor company.
- This is an opportunity to **continue building pipeline and driving leads** in partnership with our outstanding 20-year reputation and the e-Crime & Cybersecurity Congress brand.

What our sponsors say about us

SECURING FINANCIAL SERVICES

PhishRod

It was indeed a great show. Despite the situation overall [COVID 19] the number of people that turned up, shows the trust people have of the e-Crime brand. Wish you all the best for the upcoming events and we shall surely be a part of them.

KASPERSKY lab

This is always a great event for 'taking the temperature' on security issues, to get a feel for people's impressions on current security challenges and to find out what organizations of all kinds are doing.

vmware Carbon Black

AKJ has been a valuable partner for us for a few years now, enabling us to build relationships and engage with the CISO community in a number of key territories across Europe. The events they hold are a great vehicle for discussing the latest challenges and opportunities in the security sector, and our work with them has delivered way beyond expectations.

✓Ninety five percent of our exhibitors and sponsors work with us on multiple occasions each year

✓Our sponsor renewal rate is unrivalled in the marketplace

✓This is because our sponsors generate real business at our events every year

AKJ Associates