18-19 September 2018

Training Topic:
"Fraud management"

ORGANISATION SHEET

Objectives	**The key objectives of this trainings are:** ▪ fraud risk governance, people, policies & control environment, ▪ fraud risk assessment of current processes, ▪ fraud internal awareness, ▪ fraud prevention & detection solutions selection and adoption, ▪ monitoring and evaluating fraud risk management programme, ▪ fraud internal and external information and communication.
Methodology	**Introductory module:** What is fraud, common myths related to fraud, who commits fraud and what drives fraud acts. Current fraud trends. **Fraud schemes module:** Fraud typologies, warning signs and tips for internal/external frauds. Own transactions claims, first party and family fraud. Fraudulent data exchange models, fraud governance, policies and procedures, fraud target operation models examples, industry cooperation. Fraud prevention & detection software, its selection, implementation and adoption within organisation. **Tax fraud schemes module:** Most common tax fraud schemes, examples of VAT fraud schemes, **Financial statement fraud module:** Identity theft (ATO), synthetic identity, fake or farm companies, fake company registry or tax statements, non-existing assets or overevaluated collaterals, fake bids/tenders, fake sales, cooking the books, cooking management accounts and KPIs, analysing financial statements, warning signs and tips, examples and case studies.
Target group	**Main target group are employees from:** ▪ Operational risk department ▪ Credit risk department ▪ New products development, digital channels and customers remote acquisition ▪ Compliance / AML / Fraud operations ▪ Sales (Retail, Corporate, SMEs) ▪ Optional for finance and legal department employees
Language	Training will be delivered in English language.
Participants	20-25 participants
Place & Date	18-19 September 2018, Sokrat Hotel Tirana
Investment	250 Euro (including tax)

Expert BIO

Mr. Konrad Krupinski
Manager, PwC Czech Republic

Education and Professional qualifications:
Post-graduate degree, Operational Risk in Commercial Bank, University of Warsaw
Masters, Journalism & Political Science, University of Warsaw

Areas of expertise:
Financial Crime (Fraud, Cybercrime, Customers on boarding and digital acquisions, PSD2, AML, Operational Risk, BASEL, Law enforcement cooperation, Country level cooperation)

Years of Experience:13

Language skills:
Polish (native)
English (professional working proficiency)
Czech (beginner)

Experience Summary
Konrad has hand-on knowledge of financial crime taxonomies (Fraud, Cybercrime, PSD2, BASEL & Operational Risk) and solutions to detect, prevent and recover losses in banking and payments. He had served as a member for a Polish Banking Association (Cards Issuers Council) and he also was a member of MasterCard Fraud Advisory Council for EU countries. Konrad is experienced in financial crime, cybercrime and antifraud projects implementation and set-up tuning.
He specialized in fraud management policy development including credit fraud prevention/detection strategies, customer/employee fraud, funds transfers/cards transactions monitoring, customers onboarding & multi-factor authentication, transactions clearing, settlement, chargebacks, customer complaints, losses detection & loss prevention analysis, reporting, law enforcement bodies & financial supervision cooperation. Have in-depth knowledge about PSD2 & BASEL regulations and standards.

Relevant projects
Setup of the FIU in financial institution, responsible for BM reporting, fraud investigations and relationship with the state FIU & FSA
Defining and implementing financial crime risks management programs/policies in various banks and financial institutions (VP)
Implementing Financial Crime prevention & detection (internal and external threats within credit & transactions environment) solutions (e.g. KD Prevent, EDA Hunter II, Cortex, Alaric Fractals, ECS+, DC, Anti-malware, Device-Print, Polish National Lending Crime Database) in various banks and financial institutions
Leading projects with Financial Crime software vendors in the areas of credit and founds transfers fraud (e.g. KD Prevent, Fraud Hub, FDS)
Setup of PCI DSS & PSD standards across FI
Setup of 3D Secure standards across FI
Implementing changes and delivering remedial plans for fraud issues identified by state FSA, compliance testing with accordance to local law & regulations & fraud risk management programs,
Fraud and Financial Crime knowledge transfer / training (Fraud Audit, Fraud Risk Management, Organized Crime) and held lectures at various Financial Crime events (e.g. HPS, PBA).

Agenda

Day 1

Module 1 - introduction

A. What is fraud, common myths related to fraud, who commits fraud and what drives fraud acts, fraudster profile and psychology, consequences of fraud for financial institutions – financial losses, legal consequences and reputational damage.
B. Current fraud trends in areas of:
   - loans applications and place of origin,
   - account opening and customers relationship management,
   - card's transactions monitoring including CNP,
   - online banking and online payments and transfers, phishing, vishing, SWIFT fraud,
   - EU PSD2 anti-fraud transactions requirements for transaction monitoring, strong customer authentications (SCA/MFA), transaction risk based analysis (RBA),
   - EU PSD2 benchmarks and to be adopted by players within and out of EU zone.

Module 2 – fraud schemes

A. Fraud typologies, warning signs and tips for internal/external frauds related to deposit/credit products, e-banking and banking applications - examples and case studies.
B. Own transactions claims, first party and family fraud, debt through off-line transaction (NFC, AFD, TOLL, and DEPOSIT), fraudulent transfers / transactions.

Day 2

Module 2 – fraud schemes

C. Fraudulent data exchange models within banks and on country level, internal fraud governance, policies and procedures, fraud target operation models examples, industry cooperation, law changes, fraud IT tools selection, implementation, adoption and constant tuning.
D. Policies, standards and databases implementation at Association level for constant sharing of new fraud trends and/or fraudulent data.

Module 3 – tax fraud schemes

A. Most common tax fraud schemes, examples of VAT fraud schemes.
B. Technology and processes used for detection.

Module 4 – financial statement fraud module

A. Identity theft (ATO), synthetic identity,
B. Fake or farm companies, fake company registry or tax statements,
C. Non-existing assets or overevaluated collaterals,
D. Fake bids/tenders, fake sales,

E. Cooking the books, cooking management accounts and KPIs,
F. Analysing financial statements,
G. Warning signs and tips, examples and case studies.