Global and Regional Retail Fraud Advanced Topics – Ritz Carlton DIFC *Dubai Dec 6, 2018*

***Responding to new and intensifying familiar fraud threats impacting retail credit providers, merchants and any business plugged into the digitalized* world.**

Attend this informative and expert driven 1-day conference on the best practices for dealing with current and emerging fraud threats in the Middle East and from around the globe.

Learn first-hand from experts about latest trends in fraud attacks & how to optimize responses:

- Data breaches at both retail and e-commerce merchants' stores.
- Enumeration attacks by bad actors using brute-force to guess or confirm valid users in a system.
- Bogus post-authorization fraud that victimize payment-card acquirers.
- Fraudulent credits targeting online merchants whose digital defenses are compromised.
- Illegal transactions / bogus services from e-commerce merchants set up to process gambling transaction or "sell" worthless products and services
- Authentication data manipulation schemes to circumvent chip card fraud protections
- QR (Quick Response) code scams that embed viruses in cell phones to steal personal information
- BEC (Business Email Compromise) involving spoofed or compromised wire transfers
- Synthetic Identity Fraud, involving the use of fake information, such as a fictitious name, and real data to create a "victimless" fraud
- Mobile Ad Fraud victimizing internet advertisers
- Call Center Fraud designed to overwhelm and confuse customer-service staff via telephone denial-of-service attacks
- Exploiting the global glut of account data from the recent spate of massive data compromises to turbo-drive CNP (Card Not Present) and ATO (Account Take Over) attacks
- Phantom Company Fraud; Run-away Expat Fraud and Funds Transfer Fraud

Discussion with experts will be supplemented with real examples proven strategies that have proved successful in similar consumer lending environments

Course Objectives

- Provide a high-level understanding of the latest global and regional fraud attacks
- Discuss emerging fraud schemes from other regions that a likely to migrate to other regions.
- Discuss known countermeasures and best practices for dealing with fraud

Why you should attend:

- To better understand and respond to the risks in the ever increasingly digitalized world
- Understand what your organization needs to be prepared to avoid or repel fraud attacks
- Determine where your business is on the Digitizing Spectrum and what your next steps should be to optimize digitization technology.
- Get hands-on strategies and best practices for developing countermeasures to prevent or mitigate the impact of fraud attacks

Who Should Attend

- Business Managers from retail credit, card payment, merchant and any consumer businesses subject to fraud attacks on their business or customers
- Product and Marketing Managers concerned about designing and growing businesses and services subject to fraud attacks.
- Credit Risk Managers responsible to modify lending polices in response to current and emerging fraud attacks
- Operations Managers needing to respond to the new environment though changes staffing, training and technology
- Other managers needing to respond to these environmental changes:
    - Operational Risk Managers
    - Internal Audit

Planning and Forecasting Managers

Infinity Risk Advisors

Fraud Advanced Topics

Dubai, UAE Dec 6, 2018

Course Facilitator

Peter Dean has over 25 years of experience in different aspects of consumer banking risk management, with special emphasis on credit risk and fraud management. He was both the Global Director of Consumer Bank Risk Training at Citibank and its Global Director of Fraud Management.

The instructor wrote the fraud management and collections management policies incorporated into the Global Risk Management Polices. In addition, he led teams of experts that developed global collections and fraud management best practices.

Through his fraud management experience, Peter Dean has become expect at completing fraud vulnerability assessments for banks, finance companies and corporations subject to internal and external fraud attacks. He is an approved vendor for both MasterCard and Visa.

He has a BS degree from Syracuse University

Agenda

Cyber Security Essentials for Fraud Protection

- Network Security
- Endpoint Security
- E-Mail Security
- Managed Defense

Acquirer and Merchant Fraud

- Data breaches at both retail and e-commerce merchant stores
- Bogus post-authorization fraud
- Fraudulent credits targeting online merchants
- Bogus Merchants set up to:
    - Launder illegal transactions
    - Sell worthless products and services

Payment Network Attacks

- Authentication data manipulation schemes to circumvent chip cards
- QR (Quick Response) code scams that embed viruses in cell phones
- BEC (Business Email Compromise) involving fraudulent wire transfers
- ATM system-wide Cash-out attacks

Turbo-Charged Classic Attacks

- Synthetic Identify Fraud; Call Center Fraud
- Brute-force attacks access or overwhelm systems; Exploiting the global glut of compromised account data

UAE "Old Standbys"

- Phantom Company Fraud; Run-away Expat Fraud; Funds Transfer Fraud; Insider Fraud

Fees: US: **$1,495 per participant –** This includes daily coffee breaks, lunch and copies of conference presentations and materials for the days attended.
Please inquire about discounts available for sending more than one person from your organization at ayazafridi@infinityrisk.com

Go to: https://www.infinityrisk.com/rdxbfs to register