

Webinar on

Identity Issues In Banking - After The Breach, 26 Red Flags And More

Areas Covered

- *What has changed in customer identity considerations?*
- *Problems with the “26 Red Flags”*
 - Red flags indicating ID threats for new Accounts
 - On application
 - On credit reports
 - On documents provided
 - On early use of new credit
 - Red flags indicating ID threats for new accounts
- *Directions for ID Tools in a post-breach world*

This is a chance to look at existing ideas in customer identity in new ways and to consider both practical, short-term improvements as well as look at where the solutions may be evolving.

PRESENTED BY:

Jim George is an independent consultant to banks focusing on issues of identity, Know Your Customer issues, and fraud. He brings over 25 years as a consultant to major banks in Associate Partner and Principal roles at PriceWaterhouse-Coopers Consulting, IBM Consulting in Bank Risk and Compliance, and Andersen Consulting.

On-Demand Webinar

Duration : 60 Minutes

Price: \$200

Webinar Description

This is a chance to look at existing ideas in customer identity in new ways and to consider both practical, short-term improvements as well as look at where the solutions may be evolving.

The Federal regulators put together a list of 26 “Red Flags” to help banks deal with ID theft and identify fraudulent attempts to take over accounts. But the list is not organized for ease of use and they are not a comprehensive guide. In this topic we have organized the Red Flags into related functional areas and, for each area, we provide additional tips and information based on years of consulting with major banks from the perspectives of prevention, loss reduction, detection, and investigations.

Major data breaches have changed the game. They are part of a trend toward “industrializing” id and fraud crimes, so no one person has to do each step. Data is available in the Dark marketplace for small fees per victim. Old controls are less effective and we need to change just to keep up with the perpetrators.

Where do you go from here?



Who Should Attend ?

Retail Banking Leaders

Risk and Compliance Officers

Loss Control Managers

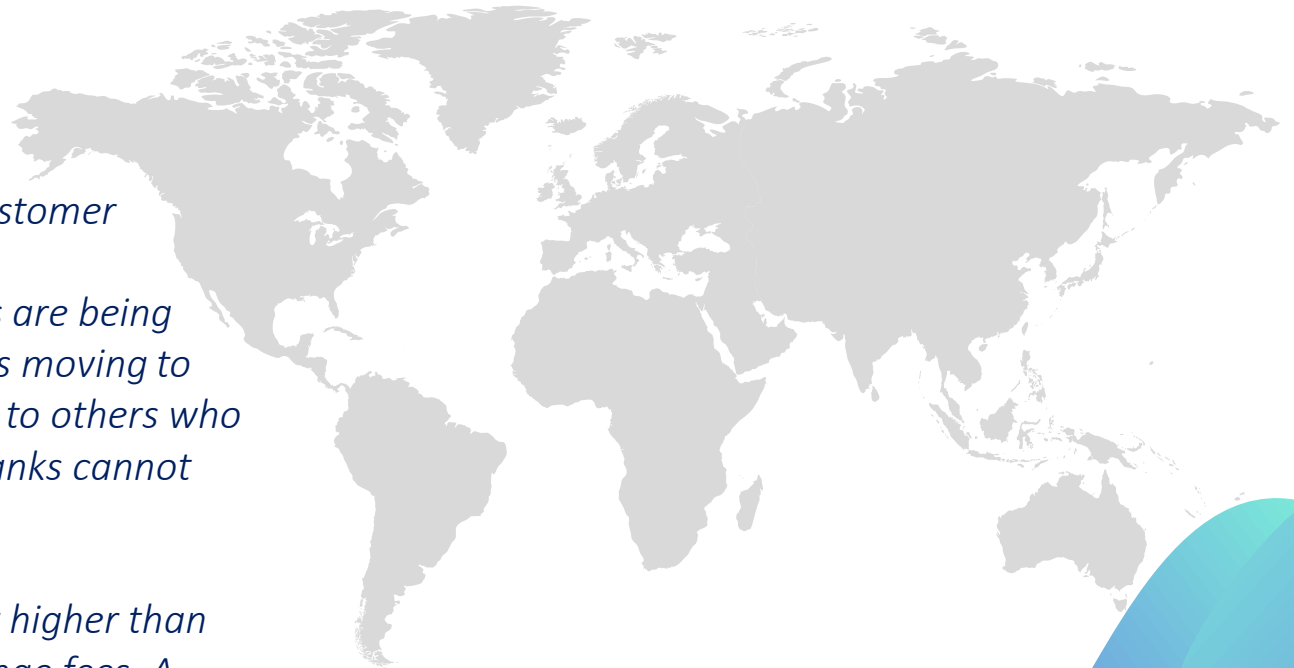


Why Should Attend ?

Fraud is of more concern to banking leaders today than ever before. This is driven by national media coverage, actual dollar losses, the attack on trust (which is key to customer relationships), costs to allay customer concerns, changing regulatory environment, and changes in how fraud efforts are being organized. Fraud is no longer just a “cottage industry”, it is moving to an industrial model where specialists steal data and sell it to others who organize high-volume attacks by multiple perpetrators. Banks cannot combat the “Fraud Industry” with yesterday’s methods.

There are reasons to believe that fraud losses are actually higher than recognized. Some fraud losses are buried in card interchange fees. A significant amount of fraud losses likely get reported in banks’ accounting as credit losses. But they weren’t due to poor credit decisions, they were fraud scams from day-one.

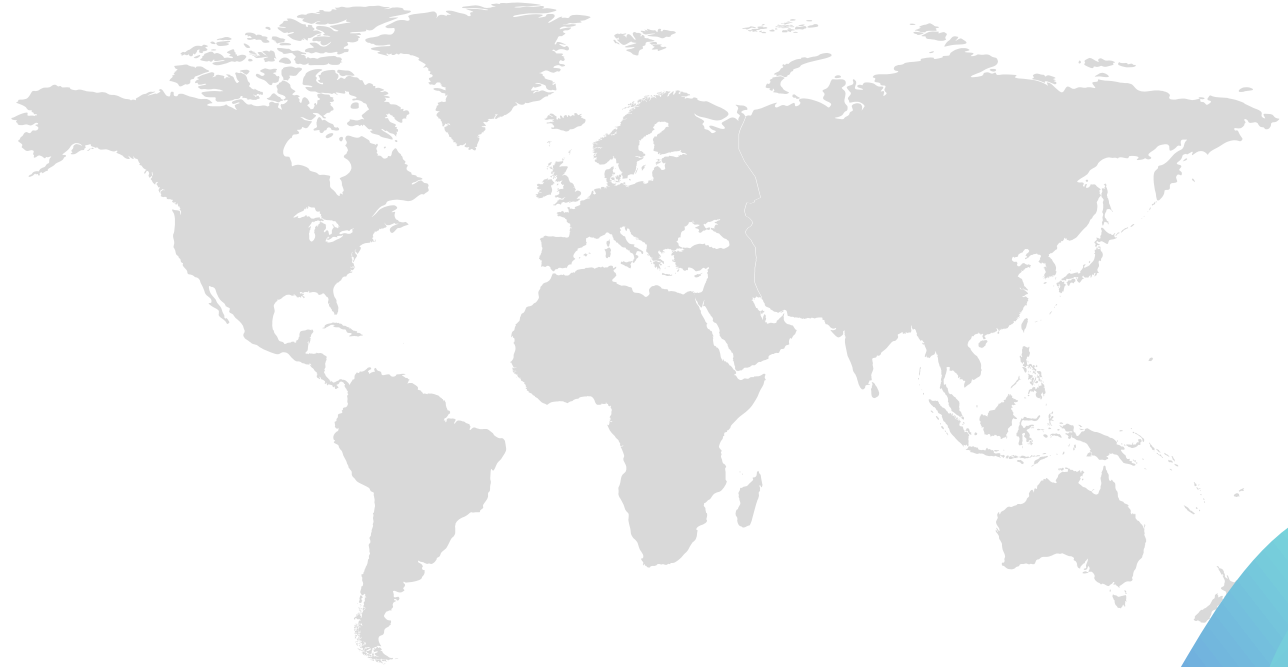
The software is widely installed to identify specific patterns and “unusual” transactions. But the fraudsters know this and are constantly striving to create new patterns where their transactions are designed not to be flagged. Like in a game of chess, the advantage goes to the side that thinks the most moves ahead.



Topic Background

What is going on with regard to customer ID and the major data breaches?

Banks have been increasingly depending on Credit Agencies' data to support their customer identity needs. After the data breach at Experian, fraudsters buying data on the Dark Web have access to the same credit report data the bank does. Banks need to do some basic rethinking about customer and potential customer identity issues. And they need to do that quickly. This is going to require creative thinking, as there is no "solution" in a box on the shelf.



To register please visit:

www.grceducators.com
support@grceducators.com
740 870 0321