WHITE PAPER

Effectively combating the new age electronic frauds

Key technology solution recommendations for FIs

Infosys
be more

Introduction

In an Infosys' whitepaper entitled, "What makes combating the new age e-frauds challenging for FIs?" the authors had emphasized on why, more than ever before, effective electronic fraud (e-fraud) management needs to be a key priority for the financial institutions (FIs). This is owing to the fact that, in recent years, across the world, the menace of e-frauds has reached alarming proportion. Today, most FIs are grappling with a variety of new age e-frauds. Consider the below statistics.

- As per the global benchmark data from ACI Worldwide and Aite Group, globally, 30% of consumers have experienced card fraud in the last five years
- According to the data from Financial Fraud Action UK, losses resulting from payment card fraud in 2016 increased by 9% YoY
- As per the ACI Worldwide benchmark data, for the holiday period between Thanksgiving and the New Year eve in 2016, global fraud attempts increased by 31% YoY
- According to a Javelin Strategy & Research Study, in U.S., identity fraud reached a record high in 2016. There were 15.4 million identity fraud victims in 2016 – constituting YoY increase of 16%

Given the gravity of the e-fraud situation, FIs need to bolster their e-fraud detection and prevention (i.e. e-fraud management) capabilities by earnestly transforming their existing ineffective antifraud technology solutions. Unfortunately, many FIs are unsure of how to achieve this. This whitepaper provides key recommendations for FIs to effectively transform their antifraud technology solutions.

Key recommendations

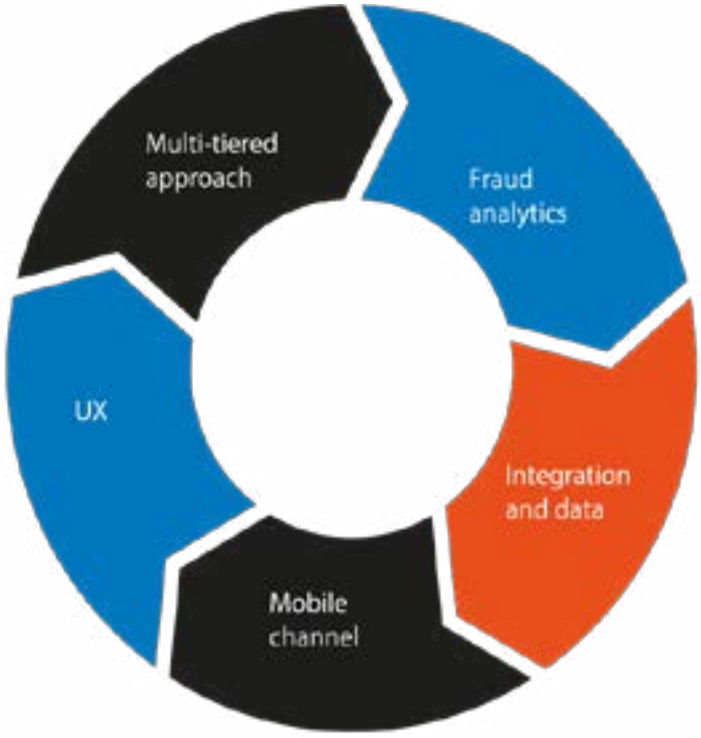


Exhibit 1 – Key recommendations for enabling robust antifraud technology solution

- **Multi-tiered approach:** Many FIs rely on a single tier solution for their e-fraud management. However, a single tier approach is grossly inadequate to combat today's tech-savvy fraudsters. It is therefore recommended that FIs adopt a risk based multi-tiered approach. Such an approach would help assess the users' digital activities at multiple levels and enable an in-depth shield against e-frauds.

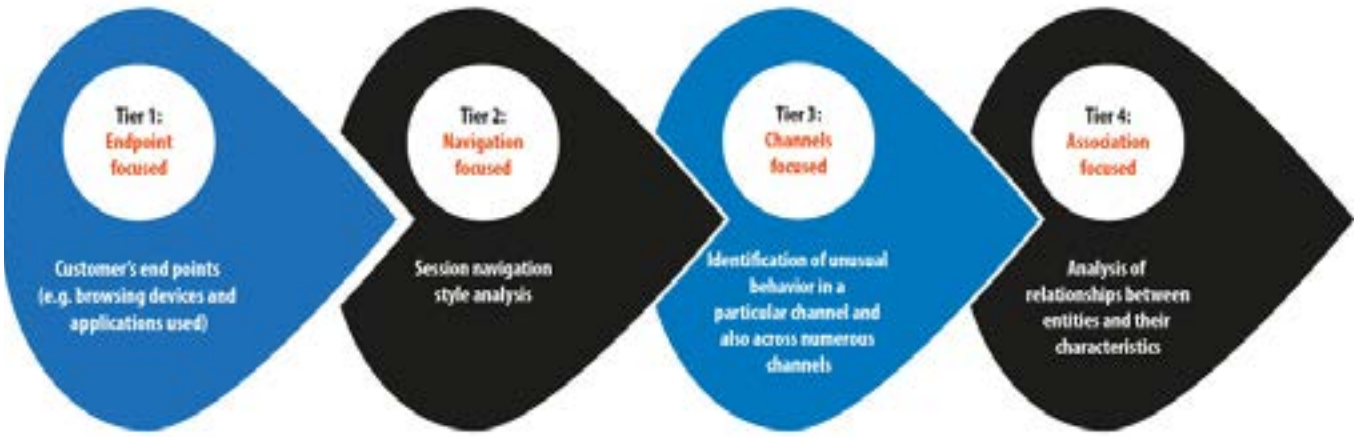


Exhibit 2 – Multi-tiered approach to e-fraud management

- Refer below the key solution characteristics of each of the four tiers mentioned in exhibit 2. An FI may choose to implement the four tiers in a phased manner.

Tier 1: Endpoint focused

- This tier helps in combating malicious software attacks – such as spyware, ransomware, computer virus, trojan horse, and adware. Solution in this tier is focused on securing the customer's access endpoint (browsing devices and application used). It involves automated analysis of the characteristics of user devices (mobile, PC, tablet etc.) that connect with the FI's systems
- In order to access FIs' digital channels, users need to go through authentication band:
  - For small-risk situations, dual-factor authentication (2FA) is enforced. Example of 2FA - combination of software ID and a personal-identification-number (PIN)
  - For large-risk situations, advanced multi-factor authentication (MFA) is enforced - including out-of-band-authentication (OOBA), 3-D Secure (3DS) tools, biometric authentication, transaction data signing devices, and making use of endpoint device characteristics (geolocation, device id etc.)
- Protected browsing via locked browsers, and browser plugins to prevent code injection are couple of additional examples through which endpoint security can be enforced .

Tier 2: Navigation focused

- This tier helps notice: a) distinct suspicious transactions, b) malicious software enabled activity (that manifests as unusually speedy navigation or an uncharacteristic navigation pattern), and c) fraudsters rings
- Solution in this tier is focused on in-depth analysis of the users' session navigation or network behavior. Real-time information gathering on customer/account online activity also is done. This is then utilized to build and continually evolve the baseline customer profiles.
- A user's particular session navigation is then compared, in real-time, against the baseline user and peer-group profiles for anomaly detection. Rules are also made use of for identifying strange navigation patterns

Tier 3: Channels focused

- This tier is focused on both: a) account- and user-centric behavior for an individual channel; and b) cross-channel and cross-product behavior of user and account
- For a) above; rules/statistical models are used; and user, account and related transactions behavior are monitored and analyzed. For anomaly detection, comparison of the specific transaction is done against continually updated profiles (user, account, all accounts that roll in under the user, peer group)
- For b) above; user and account behavior across products/channels are automatically monitored and analyzed, in real-time, and compared against concerned profiles (including the omnichannel profiles). Fraud alerts are then prioritized by making use of rules/statistical models
- Cross-channel focus helps in detecting emerging fraud patterns across channels at both the customer and account level. In order to help assess their investment needs for any new e-fraud management solution related to a specific channel or payment method, FIs should work towards establishing key metrics for cost per fraud incident for each channel and payment methods

Tier 4: Association focused

- This tier helps to:
  a) Identify behavior patterns that appear to be dubious only when analyzed across related individual/organization and accounts
  b) Discover networks that are associated with suspicious individual, entity or account
  c) Gain holistic assessment of related entities and customers and their relationships
- Solution in this tier analyzes the links amongst the internal and outside entities and their characteristics. For example, characteristics related to users, devices, computers and accounts are all analyzed to detect complicit or coordinated fraudulent activities. Focus is on analyzing entire relationships and activities within the individuals/entities network (for example, customers having similar demography)

- **Fraud analytics:** In order to gather deeper insights, develop actionable intelligence and enable automated responses to fraud, FIs need to leverage robust fraud analytics capabilities. A hybrid fraud analytics approach, comprising a combination of the basic and advanced analytics capabilities can be adopted. Further, where appropriate, FIs can consider leveraging new-age artificial intelligence and machine learning enabled solutions as well.

Approach type	Fraud analytics approach	Key characteristic	Suitable for	Example
Basic	Rules based	Rules for filtering fraudulent behaviors and transactions	Known patterns	• Transaction by a user in different time zones in a short time frame
	Anomaly detection based	Can detect individual and aggregated anomalous patterns	Unknown patterns	• Accounts per address exceeding norm • Wire transactions on account exceeding norm
Sophisticated	Advanced analytics	Predictive fraud assessment using advanced models	Complex patterns	• Complex account closing and opening pattern or wire transaction pattern

Exhibit 3 – Hybrid fraud analytics approach for e-fraud management

Powerful advanced fraud analytics can enable severable benefits to FIs. Refer below exhibit.

Key features of advanced e-fraud analytics

Fraud models evolution

- **Deployment, monitoring and support of multiple fraud models** and modeling tools (pattern recognition, neural networks, predictive etc.)
- Robust modeling platform and **machine learning enable continual self-calibration and evolution** of fraud scoring and predictive models
- **Text and visual analytics inputs** aid model evolution
- **Leading industry tools (such as IBM SPSS) support execution** of runtime models
- **100% real-time scoring** of authorizations and transactions
- **Statistical analysis** for creating custom thresholds
- **Sensitivity analysis** for tuning of alerts in real-time

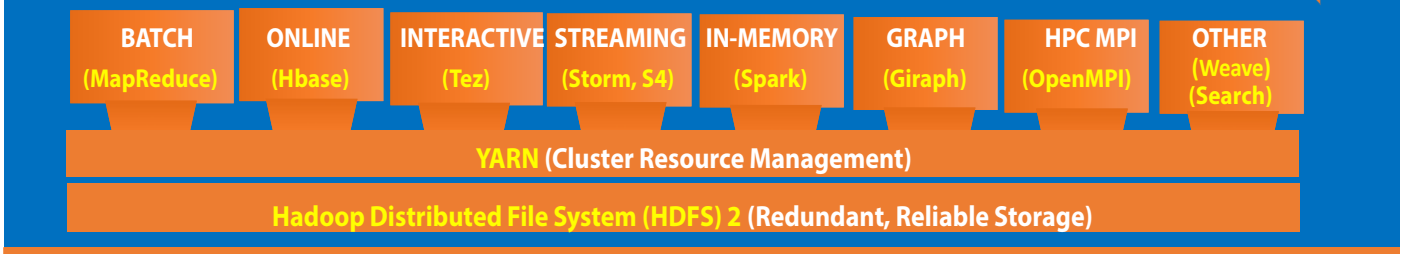
Behavioral profiling, linkage analysis, and decisioning

- Continual and **adaptive behavioral profiling and segmentation scheme**
- **Linkages across key attributes** (name, address, email address, device, phone, IP etc.) to uncover suspicious patterns
- **Proactive identification of entities and practices** associated with various e-fraud types
- **Decision engine for real-time and automated decisioning** based upon transaction scores
- **Real-time transaction screening**

Big data capabilities

- **Real-time analysis of very large data sets**
- **In-memory analytics engine** for real-time streaming and analysis of structured and unstructured data
- **Real-time integration of streaming data** with the historical information
- **Tools such as Apache Hadoop** (an open-source framework for distributed storage and processing of big data) **enable highly scalable data processing**

Hadoop: native applications



Application	Salient aspect
MapReduce	▪ Programming model for **processing/generating big data sets via parallel processing** ▪ **E**nables **flexibility, scalability, speed, and cost effectiveness**
Hbase	▪ The open source, distributed, non-relational database enables **a) low-latency data access and fast processing of billions of records, b) consistent read/write access in high volume request, c) auto failover and reliability**, and more
Tez	▪ **Helps meet demands for extreme throughput and fast response times** at petabyte scale
Storm	▪ Enables **reliable real-time processing of unbounded data streams**
Spark	▪ The high speed data processing engine **enables in-memory data processing and sophisticated analytics**
Giraph	▪ Enables **iterative graph processing** and is highly scalability
OpenMPI	▪ Enables the **best High Performance Computing (HPC) Message Passing Interface (MPI) library**
Weave / Twill	▪ Its simple programming model and reusable components **enables easy harnessing of the power of YARN**

Exhibit 4 – key features of advanced e-fraud analytics

- **Integration and data:** FIs should work on integrating their fraud management and cybersecurity capabilities. Further, they should leverage integrated fraud management solution that covers broad spectrum of financial crimes across all of the digital channels; and which enables configurable integration of data and workflows. Fraud management solution should also be effectively integrated with FI's CRM, financial processing (e.g. transaction authorization, payments engine), AML, core systems, enterprise messaging and alert management systems.

  Integration of disparate data sources – both structured and unstructured - encompassing all relevant transactional, customer and institutional data is imperative. Solution that integrates streaming information with historical data should be adopted. For data integration, FIs should adopt a flexible and extensible framework and leverage the application programming interface (API) ecosystem. Focus of FIs should be on empowering their e-fraud management teams with a unified view of all of the customer's relationships and activities with the FI. To achieve this, relevant data from myriad data sources can be fed into a large data warehouse. Ready access to personally identifiable Information (PII) such as name, date of birth, Social Security number (SSN) and also non-PII information such as Internet Protocol (IP) address and device ID is also crucial.

  Integration with global or external fraud related data sources is important. Financial crime library, government records, identity repositories of credit bureaus, fraud threat and identity intelligence databases from third party vendors, PII records from data aggregators, and social network data sources are few examples of such global or external data sources. FIs may also consider forming consortium to share relevant fraud data – in addition to sharing information on antifraud protocols, techniques and standards - amongst themselves. This would help them in ensuring robust identity proofing, in quickly identifying new e-fraud threats, and in optimizing their e-fraud management strategies.

  The focus of FIs' fraud related systems and data integration undertakings should be to enable real-time decision making for effective e-fraud management and achieve related SLA compliance.

  For robust fraud management reporting, FIs can leverage consolidated reporting engine and platform. Pre-packaged reports can be leveraged, where appropriate – for example, for reports related to cases and alerts by scenario, disposition, jurisdiction, and weekly or monthly trends; and the standard management and regulatory reports. Solution should also enable robust alert and query capabilities – including ability to conduct status inquiry, blacklist, provision account history or originator reference detail etc. Further, in addition to internal systems, solution should be capable of providing alerts from external systems (such as Early Warning System (EWS), FraudNet, and CHEXSystems) as well.

- **Secure mobile channel:** While all recommended aspects (multi-tiered approach, systems and data integration, fraud analytics, and user experience) are applicable to all of the digital channels (including desktop and mobile), FIs should pay additional focus on securing their mobile channel. This is owing to the fact that, mobile channel presents significantly more avenues for fraud perpetration and the related security challenges for FIs than any other digital channels. Refer below the key elements that FIs should focus on for securing their mobile channel.

Key elements	Elaboration
	**Tracking** ▪ **Track mobile and online channels separately**, as these channels have separate security approaches and issues. Tracking these together may not bring out the issues that are specific to the mobile channel ▪ Enable **robust fraud monitoring and detection for both the mobile browser and apps**
	**Behavioral pattern** ▪ Capture and **generate anew the customer profiles and patterns that are specific to the mobile channel** – rather than simply relying on the existing ones from other channels such as PC ▪ **Evolve fraud analytics for the mobile channel.** For e.g., typical PC based device characteristics such as static IP addresses may no longer apply to mobile channel. **Leverage unique smartphone specific data such as GPS receiver, accelerometers, SIM card information, device ID and type, mobile phone tower information** etc. in fraud analytics ▪ Focus on **tying together an individual's device inventory (mobile, tablet, PC etc.)**
	**Advanced authentication** ▪ Where feasible, **leverage biometrics based authentication** – such as device fingerprinting, iris scan, facial recognition and voice recognition ▪ Where appropriate, **adopt passive biometric techniques that enables "behind the scene" analysis.** For e.g., using this technique, over time, system gets trained on a customer's biometric "signature". A particular biometric authentication attempt can be then compared against this customer's biometric "signature" to ascertain if the said customer is in fact being impersonated by a fraudster using his device
	**Mobile SDK** ▪ Leverage **robust mobile security software development kit (SDK) that helps embed strong security features** within the mobile apps and gather real-time threat intelligence ▪ For example, for secondary authentication, **such an SDK could create unique device ID for every customer device.** It could also help **gather intelligence on applications running, rooted/jailbroken status, keyboard running, if device is running in emulator, geo location, network information** etc. ▪ Enable **such SDK for all major mobile operating systems** (iOS, Android etc.)
	**BYOD** ▪ **Address security threats that Bring Your Own Device (BYOD) policy for FIs' employees pose**, when these employees connect their devices to access the FI's data

Exhibit 5 – Key recommendations for e-fraud management on mobile channel

- **Focus on user experience (UX):** FIs' e-fraud management solution should not lead to negative customer experience. To the extent possible, the solution should be non-intrusive. For example, FIs can make more usage of back-end technology controls, which monitors suspicious activity in the background and without customer's knowledge. Similarly, more real-time checks, without the need for user interaction, can be enforced – by utilizing already available data points such as historical or device related information. Additionally, FIs should remain focused on rendering maximum fraud detection and prevention and at minimum false positive rates. Further, FIs need to provide their e-fraud management teams as well a "frictionless" experience. Refer below few UX enablers that apply to e-fraud management solution.

Dimension	UX enabler
Tools 	▪ **Graphic and visualization tools for analysts** – that shows contextual correlation, data outliers and patterns, network visualization, simulation etc. ▪ **Graphical dashboard** that classify profiles based upon high, medium, or low risk ▪ **Executive e-fraud dashboard** – that provides configurable and graphical line-of-business or enterprise level views against KPIs ▪ **Analytics GUI** to manage statistical models ▪ Tool for seamless **real-time hot-listing** ▪ **Robust forensic tools** for e-fraud investigation ▪ **Configurable and flexible rules engine** ▪ **Automated workflow and task assignment** to fraud investigative team ▪ **Tools for easy setting of parameters** - account activity thresholds, transaction scoring related etc. ▪ **Multi-language support**
Case management 	▪ **Robust case management tool** that: ❖ Enables **360-degree view** of all of the financial crime investigation data, cases and alerts ❖ Enables **graphical visualization of the case** ❖ Presents **consolidated view of additional cases, assessments and compliance alerts** that involve the same or related users/entities ❖ Provides **ability to speedily share, via standardized formats, individual cases and alerts** across all fraud, financial crime and compliance systems
Alerts 	▪ Efficient **alert prioritization and routing mechanism** ▪ Flexible tool for creating various **customizable alert types** (text, email, or app-based) ▪ Insightful alerts – **includes details on the questionable transaction and clear action recommendation** to dismiss or remediate
Authentication 	▪ **Frictionless authentication** ▪ Can **dynamically change the degree of authentication required** – depending upon factors such as geolocation, log-in time, network used etc. ▪ **Sophisticated failover mechanisms** for ensuring that one-time passwords (OTPs) are always received ▪ **Adaptive OTP delivery methods** depending upon user's login context such as location ▪ Provides **status feedback** that allows user to easily follow the log-in progress, without needing to call the FI's helpdesk

Exhibit 6 – UX enablers of e-fraud management solution

Bringing it all together…

Refer below a conceptual view that illustrates some of the key elements of a robust e-fraud management solution.

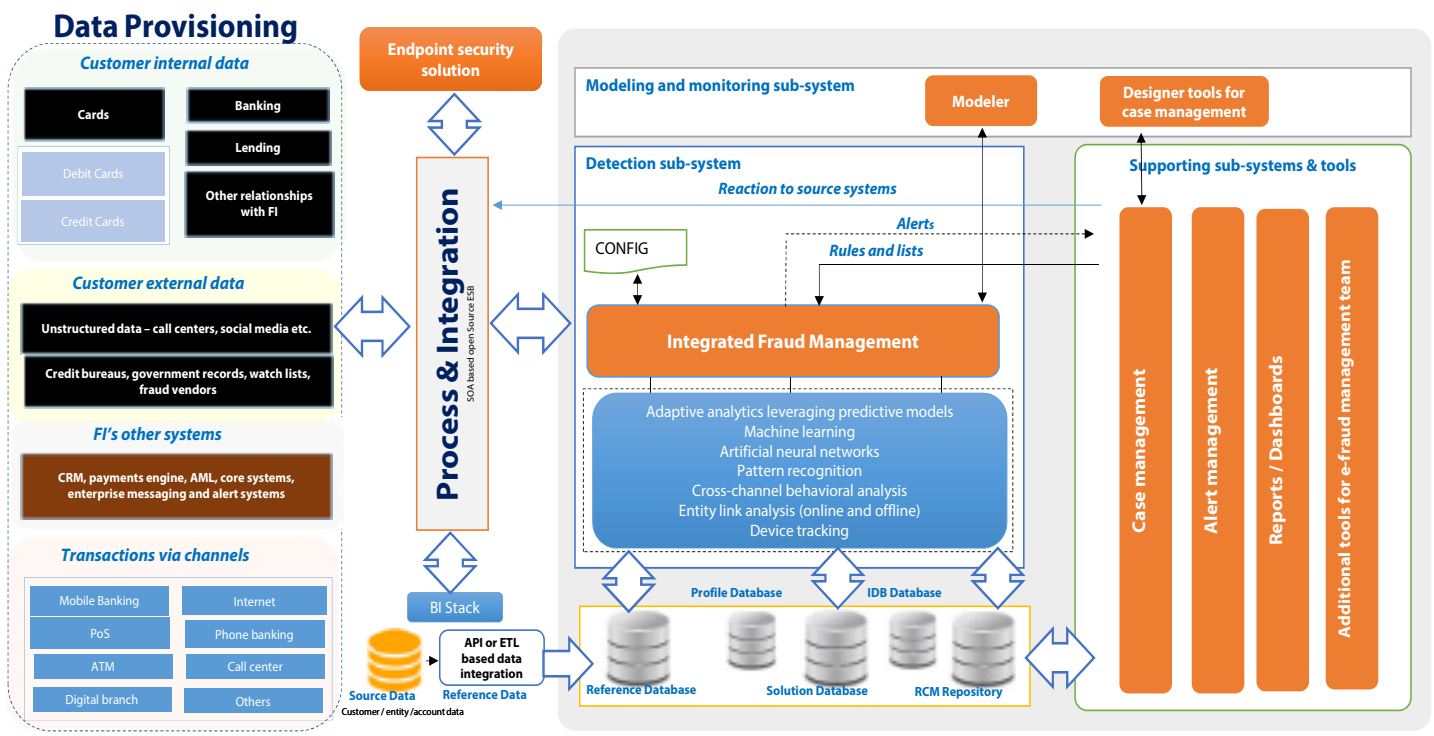


Exhibit 7 – A conceptual view of recommended e-fraud management solution

Real-world examples of robust e-fraud management capabilities

Securing mobile channel

Jibun Bank, which is a Japanese mobile-focused internet bank, secured its online and mobile banking channels and transactions using VASCO's Transaction Signing Solution. The bank leveraged VASCO's VACMAN Controller along with DIGIPASS for Apps.

DIGIPASS for Apps SDK is a complete library of multifarious security solutions which developers could embed natively into a self-developed mobile application. Using this SDK, Jibun Bank has launched transaction signing feature in which a value of transaction is seamlessly transferred in the application. In this highly secure and smart setup, customers don't need to worry about typing in a lot of transaction details.

Securing e-payment

Bottomline Technologies launched a new payment fraud solution for the SWIFT payment network members. The network includes some of the world's largest FIs. The solution – which is available on both cloud and on-premises – goes above and beyond the mandatory controls; and includes real-time monitoring of individual messages and user behavior in order to stop potentially fraudulent payments.

SWIFT has introduced a real-time payment controls service to help banks spot fraudulent messages. Banks can integrate this service directly with their SWIFT messaging flows, thereby making it easier for them to detect unusual patterns, and screen messages as per their firm's specific risk and compliance policies. The solution can learn users' transaction patterns and "red flag" non-compliant payment messages. It can also build a profile of the bank's message traffic - based on their business activities across counterparties, countries and currencies.

Emerging fraud threats identification through consortium data

Nice Actimize has introduced ActimizeWatch, which is a cloud-based solution for fraud analytics optimization. ActimizeWatch uses consortium data for detecting fraud attacks before these spread from one FI onto another. It constantly monitors anonymized transactional data that are captured from a diverse range of FIs, and uses machine learning for identifying emerging fraud threats and patterns.

Securing CNP transactions

CA Technologies has launched CA Risk Analytics Network - payment industry's only card issuer network which stops the card-not-present (CNP) fraud promptly for the network members. The cloud based solution leverages global transaction data, real-time behavior analytics, machine learning, and new advanced neural network modeling capabilities to protect 3-D Secure (3DS) CNP transactions and significantly reduce losses through online fraud.

In conclusion

Given the immense challenges that the new age e-frauds pose, FIs need to, in earnest, transform their existing outdated e-fraud management approaches and fragmented antifraud technology solutions. A comprehensive e-fraud management approach is required, and which is powered by robust and holistic antifraud technology solution.

With such a transformation, FIs would be able to proactively and effectively address the new age e-fraud menace – across all of their customers' touch-points and relationship lifecycle stages. This would lead to significant reduction in fraud losses for the FI and a much more satisfied and loyal customer base. Not just that, this transformation would also help FIs significantly reduce their overall e-fraud management cost – owing to the considerable increase in fraud management teams' productivity, and substantial reduction in total cost of ownership (TCO) of the new e-fraud technology solution.

About the Authors

Amit Khullar

Industry Principal, Risk and Compliance Practice, Financial Services Domain Consulting Group, Infosys

Amit is responsible for practice management for the Risk & Compliance domain, and is engaged in solution consulting and delivery management for transformational initiatives across various Infosys clients.

He has close to 18 years of experience across the financial services industry and IT consulting. Over the years, he has managed many complex business transformation programs and initiatives for global financial institutions across the banking, capital markets, risk management and regulatory compliance segments. He can be contacted at Amit_Khullar@infosys.com

Anjani Kumar

Principal Consultant, Risk and Compliance Practice, Financial Services Domain Consulting Group, Infosys

Anjani has over 19 years of comprehensive IT, domain and process consulting experience. Over the years, he has provided consulting services and managed many large and critical IT engagements for key clients. Currently, he manages several strategic initiatives including the Competency Development Program and Thought Leadership showcasing efforts.

In the past, Anjani was also recognized as the lead process auditor for the IT division of a major global bank. He has extensive techno-functional skills and an in-depth understanding of quality and process models – CMMI, Six Sigma, ITIL, etc. He can be contacted at anjani_kumar@infosys.com

References

https://www.aciworldwide.com/-/media/files/collateral/trends/fighting-online-fraud-an-industry-perspective-volume-3-us-5227-1213.pdf

https://feedzai.com/wp-content/uploads/2015/10/Feedzai-Whitepaper-Modern-Payment-Fraud-Prevention-at-Big-Data-Scale.pdf

https://www.slideshare.net/vivastream/sas-a-layered-approach-to-fraud-detection-and-prevention

http://www.fraudconference.com/uploadedFiles/Fraud_Conference/Content/Course-Materials/presentations/22nd/ppt/9K_Subramanian_Da_Silva_Jones.pdf?bcsi_scan_94a977aee9df674a=0&bcsi_scan_filename=9K_Subramanian_Da_Silva_Jones.pdf

https://www.sas.com/en_us/insights/articles/risk-fraud/five-trends-in-fraud-solutions.html

https://www.rsa.com/en-us/products/threat-detection-and-response/endpoint-threat-detection-and-response

http://www.oracle.com/us/industries/financial-services/fs-fraud-management-br-2638108.pdf

https://www.aciworldwide.com/-/media/files/collateral/trends/preventing-money-laundering-and-bank-fraud-in-the-banking-industry-cs-us.pdf

http://www.pymnts.com/news/security-and-risk/2017/ai-fraud-fighting-machine/

https://www.finextra.com/finextra-downloads/featuredocs/jibun-bank-secures-with-vasco-case-study.pdf

https://www.finextra.com/pressarticle/68873/bottomline-ups-security-for-swift-member-clients/transaction

https://www.finextra.com/pressarticle/68904/nice-actimize-taps-consortium-data-for-fraud-analytics-optimisation-tool

https://www.finextra.com/newsarticle/30425/swift-introduces-tool-to-help-banks-spot-fraudulent-messages

https://www.financialfraudaction.org.uk/news/2016/09/20/financial-fraud-incidents-up-53-per-cent-in-first-half-of-2016/

https://www.onthewire.io/phone-fraud-jumps-113-as-criminals-focus-on-call-centers/

https://www.theguardian.com/uk-news/2017/jan/24/uk-fraud-record-cybercrime-kpmg

https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new

https://hadoopecosystemtable.github.io/

https://hortonworks.com/blog/how-big-data-is-revolutionizing-fraud-detection-in-financial-services/

https://www.lexisnexis.com/risk/downloads/whitepaper/NXR01771-0.pdf

https://www.cso.com.au/mediareleases/29577/new-ca-technologies-payment-security-solution/

http://www.biometricupdate.com/201705/daon-integrates-identityx-authentication-platform-with-experians-fraud-and-id-solution

https://www.aciworldwide.com/news-and-events/press-releases/2017/january/global-fraud-attempts-increased-by-31-during-holiday-shopping-season

https://www.aciworldwide.com/news-and-events/press-releases/2016/july/globally-nearly-1-in-3-consumers-victimized-by-card-fraud

https://www.financialfraudaction.org.uk/news/2017/03/30/financial-fraud-data-for-2016-published/

For more information, contact askus@infosys.com