WHITE PAPER

WHAT MAKES COMBATING THE NEW AGE E-FRAUDS CHALLENGING FOR FIS?

Abstract

Decoding the hurdles faced in war against electronic frauds

Infosys®
Navigate your next

Introduction

In recent years, across the world, the menace of electronic fraud (e-fraud) has reached alarming proportion. Most financial institutions (FIs) have been grappling with a variety of new age e-frauds. New types of e-fraud keep spawning with unprecedented regularity. Refer some of the alarming facts from recent times.

- In 2016, IBM discovered a new malware - GozNym - that had stolen, in just a few days of its release, USD 4 million from over 24 American and Canadian banks. The fraudsters had pooled code from two malware types, Gozi and Nymaim, to create the new powerful, persistent and extremely stealthy, chimera Trojan.
- As per the data from IBM's X-Force Research team, in 2016, over 200 million financial services records were breached. This amounts to over 900% increase from the year 2015. The data showed that the financial services industry was attacked the most – 65% higher than the average institutions across all industries.
- According to FICO, in U.S., in comparison to 2015, the year 2016 saw 70% more payment cards getting compromised at merchant card readers and ATMs that were monitored by the FICO Card Alert Service.

eCommerce growth, increased electronic flow of money, explosion of newer payments channels, rise in number of extremely tech-savvy fraudsters, and increased instances of data breaches that contribute to identity data thefts, are all key factors that have led to the rise in e-frauds. Today fraudsters leverage many sophisticated e-fraud techniques. Refer exhibit for examples.

Phishing	**Malware**	**Sophisticated advanced persistent threat (APT) style campaigns** (e.g. Carbanak)	**SIM swap fraud**	**Vishing**	**Smishing**
Account takeover	**Infiltrated point-of-sale (POS) systems**	**Identity theft** (SSN, medical identity, passport etc.)	**Social engineering scams**	**Visual spoofing**	**Spear phishing**
"Man-in-the-middle" fraud	**Content injection**	**Credit files theft** (via credit reference agencies)	**Pharming**	**Whaling**	**Skimming**
Courier scam	**Clean fraud**	**Botnet fraud**	**Gift card** (e.g. iTunes) **fraud**	**New account fraud**	**IP addresses attacks**
Software (e.g. FraudFox VM) to circumvent fraud detection techniques – such as transaction velocity and IP addresses checks, endpoint devices identification	**Chargeback fraud**	**Distributed denial of service (DDoS) attacks**	**Affiliate fraud**	**Triangulation**	**Advance fee fraud**

Exhibit 1 – Examples of e-fraud and cybercrime methods

Frauds cost FIs dearly…

At a time when FIs are relentlessly focused on reducing their cost-to-income ratios; fraud adversely affects their financial performance. For FIs, apart from the direct financial losses, fraud leads to reputational damage, decline in market share, loss of customer and investor confidence, adverse impact on customer experience, and productivity loss (owing to additional effort required for reissuing payment cards, and in analyzing and responding to fraud incidences etc.). Fraud also increases FIs' operational cost, creates opportunity costs from service disruptions, and significantly raises the risks of regulatory fines. Abnormal customer attrition rates of FIs post the fraud incidences rank second amongst all industry verticals – trailing only the pharmaceutical firms. Major e-frauds also adversely impact the entire electronic payments value chain, cutting across geographies.

As per the Global Fraud Attack Index, fraud related costs continue to rise. The rate of fraud attacks rose by 62% between Q3 2015 and Q2 2016. Further, at the start of 2015, the estimated loss due to fraud for retailers was USD 2 for every USD 100 they made. However, by Q2 2016 this figure had risen significantly to over USD 8 for every USD 100 made by retailers. According to 2017 Global Fraud & Cybercrime forecast from www.rsa.com, in 2016, phishing alone cost global firms an estimated losses of USD 9.1 billion. In Q2 2016, a new phishing attack was launched every 30 seconds.

Challenges faced by FIs in combating fraud

Given the alarming proportion that e-frauds have reached, it is no wonder that impacted FIs are desperately looking at ways to address this menace. However, such FIs face key challenges in their antifraud endeavor.

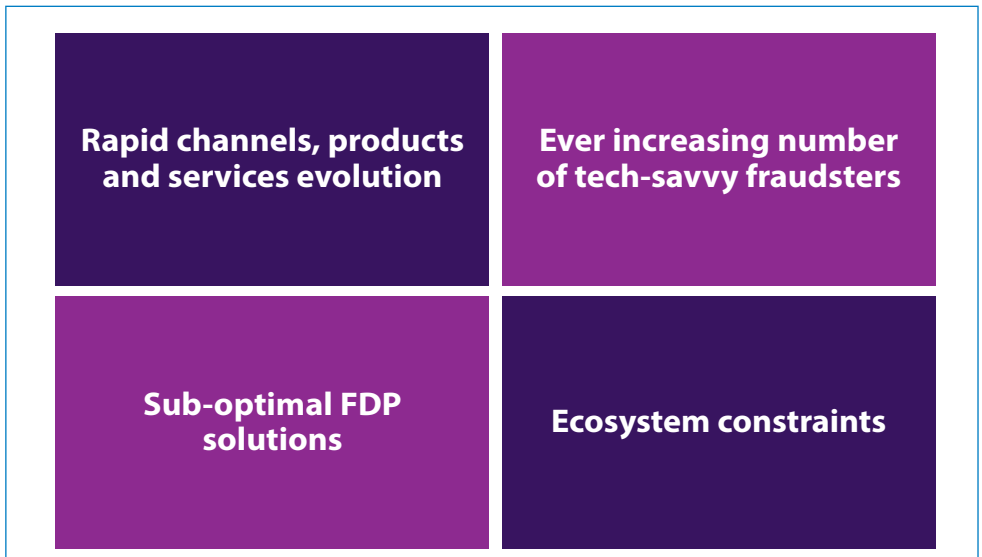


Exhibit 2 – Challenges faced by FIs in combating e-frauds

- **Rapid channels, products and services evolution:** FIs' payments channels, services and products offerings are evolving at a rapid pace. New offerings keep emerging at breakneck speed. All payments ecosystem players – including banks, alternative payments providers, card issuers, card networks, and e-commerce companies – are launching new offerings at a heightened frequency. Such rapid evolution of offerings add to FIs' fraud management challenges. For example, when Apple Pay was launched, it gave customers a convenient means to pay their retailers directly via their smart phones. However, even though this new payment mode increased customers' convenience, it also led to new fraud related vulnerabilities for FIs. Fraudsters were able to load stolen cards on iPhones for making purchases via Apple Pay. With regards to this issue, security analysts opine, it would have been better if issuers had enforced more due diligence at their end for ensuring identity proof. However, it is quite likely that issuers, in their rush to on-board the Apple Pay bandwagon, had overlooked implementing certain security best practices at their end.

  Payment channels (such as Fedwire, SWIFT, ACH, SEPA and electronic funds transfers); online, mobile and tablet banking platforms; social platforms; unsecured employee devices and electronic gift cards are just few of the many avenues that e-fraudsters are exploiting today with impunity. Newer channels such as mobile, tablet and social platforms are found to be even more vulnerable to e-frauds. Research has shown that the cost of online fraud via mobile channel is higher than through the other payments channels. As per the www.rsa.com 2017 Global Fraud & Cybercrime forecast, while 45% of transaction volume today are initiated via mobile devices, 60% of overall frauds today originate via the mobile channel. As per RSA Anti-Fraud Command Center, in U.S., in comparison to 2014, in the year 2015, the number of e-frauds via mobile devices increased by 142%. However, during the same period, web-based fraud increased by only 3%. The exhibit below illustrates the key e-fraud challenges that FIs face from their mobile channel.

Fraud challenges for FI that mobile channel pose

More options for fraud

In comparison with other channels, mobile channel present more options for fraud. For example, fraudsters can:

- **Take over target's accounts** via mobile banking apps
- **Register stolen cards** onto mobile wallets
- Conduct **SIM swap fraud.** This fraud, which is currently quite difficult to detect, involves cancelling and re-activating new SIM cards to hack into a customer's bank accounts
- **Disable SIM cards** in victim's phone, and then divert one-time passwords via text messages onto their own phones
- Use **retailers' mobile apps for making fraudulent payments**

Sub-optimal security

In contrast to traditional PC security, mobile channel's security features are less robust. For e.g., on smartphones and other mobile devices:

- Advanced **security software usage is less common**
- There is **lack of anti-virus software usage**
- **Operating systems are updated less frequently**
- **Lack of certain features such as pop-ups and frames** on mobile browsers make 3-D Secure (3DS) adoption challenging; and **low usage of 3DS** makes the transaction insecure
- Many of the mobile **social networking and financial apps lack detailed privacy safeguards**
- Most FIs treat their mobile channel the same way as their other channels – **specific focus on addressing mobile channel security vulnerabilities is lacking**

New challenges

Owing to the following inherent characteristics of this channel, securing mobile banking present new challenges:

- **Limited authentication mechanism**
- **Data sharing vulnerabilities**
- **Public Wi-Fi usage**
- **Third party apps downloads** (this increases vulnerability to malicious apps)
- **Higher probability of device and data loss**
- Increased **vulnerability from jailbroken or rooted devices**
- **Fraud risks for Card Not Present (CNP) online and mobile transactions increase significantly** over a period of time in a region, when EMV (chip and pin) cards are rolled out in that region. As per Europol's intelligence, in Europe, in 2011 nearly 60% of payment card fraud losses, which amounted to 900 million Euros, were caused due to CNP frauds. As EMV cards make it more difficult for fraudsters to commit Card Present (CP) transaction frauds at the point-of-sales(POS)), fraudsters start attempting more online CNP transaction frauds

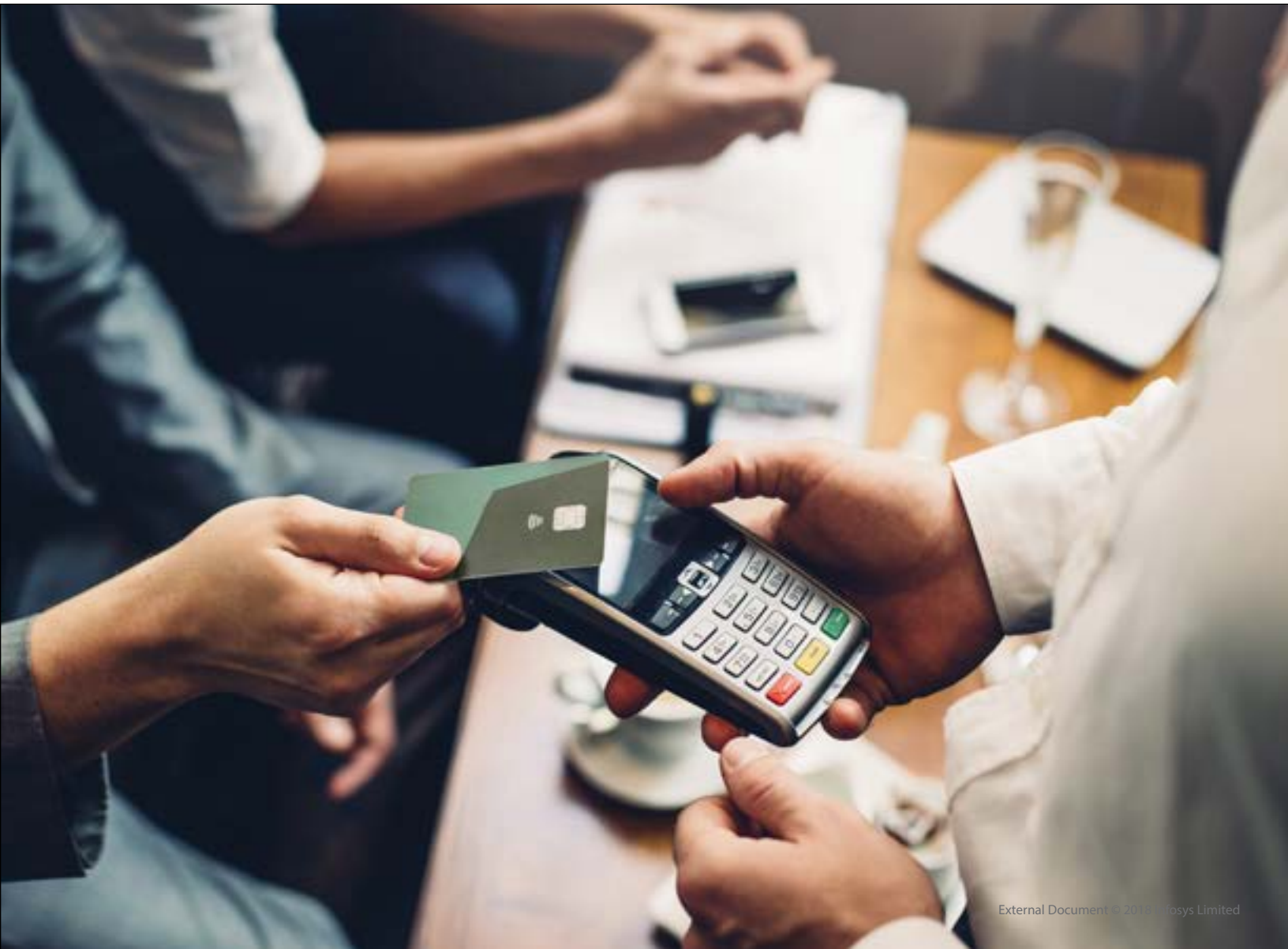
Exhibit 3 – Fraud challenges for FIs from mobile channel

- **Ever increasing number of tech-savvy fraudsters:** Today's fraudsters are super adept at outwitting FIs and utilize sophisticated software to perpetrate cross-channel frauds. As an example, in very short span of time, they are able to extract portions of code from various malwares to come up with a new much more dangerous malware. New fraud detection and prevention (FDP) solutions that FIs implement are made vulnerable, or alternative fraudulent means identified by crooks in almost no time. For proof, refer the considerable increase in botnet and other automated fraud methods in recent times, and the significant rise in online CNP frauds post the EMV implementation in certain geographies.

  Fraudsters today have also become expert at mimicking legitimate customer behavior; thereby making it harder for FIs to notice the fraudulent patterns. They actively mine various social media sites, and are able to breach FIs' other external and internal data feeds to build complete and accurate identity information on victims and perpetrate fraud. A significant surge in account application fraud can be attributed to this phenomenon. Fraudsters have also become much more organized and operate via fraud rings that span across countries. Additionally, today, fraudsters are extremely focused on exploiting FIs' internal security vulnerabilities as well. For example, many FIs' employees' computers have high security vulnerability. Fraudsters attack such employees' computers using massive waves of phishing campaigns and successfully plant malwares. As per an IBM study, 58% of the breaches tracked by IBM had its genesis in such insider attacks.

- **Sub-optimal FDP solutions:** Many FIs' existing FDP solutions are unable to keep pace with the variety, volume and velocity of the new age e-fraud threats. These solutions - especially those of the large retail banks - were built years ago using proprietary technology, and which are no longer fully supported. Many FIs have myriad disparate and inflexible FDP systems that were acquired over the years through their many mergers and acquisitions.

  Studies have found that the overall fraud levels are high even in countries where FDP solutions are pervasive. To add to the woe, in recent years, after being acquired by larger firms in adjoining markets, some of the leading FDP solution vendors have lost their focus and ability for breakthrough innovations.



Examples of issues with FIs' existing FDP solutions	
Absence of omnichannel support	
	• **Lack easy configurability** to support emerging omnichannel needs • **Unable to monitor customer behavior across multiple channels,** products, accounts and systems. For example, transaction data are not encoded with a tag to recognize the channel used • **Unable to provide accurate measurements of fraud metrics by sales channel**
Sub-optimal integration	
	• **Lack robust integration with transaction systems and enterprise applications and tools** • **Unable to provide single-customer and enterprise-wide view.** There is lack of sound data integration with concerned lines of businesses' (LoBs') systems. LoBs' data don't get optimally fed into the FDP systems and risk engines
Don't leverage social data	
	• **Ill-equipped to automatically leverage social media** feeds to combat fraud. As an example, customer information gathered by the marketing systems from **social log-in data feeds are not fed into the FDP decision engine** • Many FIs **assess social profiles via ad-hoc and time-consuming manual review process** • Many other FIs, **even though they collect information from social platforms, don't leverage it much** in their antifraud endeavors
Lack in scalability and predictive abilities	
	• Today, global FIs process tens of millions of transactions on hourly basis. FIs' **existing FDP solutions are unable to effectively support such high transaction volume** and dynamic requirements • Rules are based on past fraud patterns; and hence **unable to predict new types of future attacks**
Need manual intervention	
	• Are **based on primitive rules that are difficult to manage**, and require extensive manual reviews of fraud incidents. This leads to significant resource overhead and incidents analysis delays • As per a Juniper research whitepaper, for merchants using FDP solutions to flag fraud, **three-quarter of the flagged transactions are eventually resolved through manual reviews by internal staff**

Exhibit 4 – Examples of issues with FIs' existing FDP solutions

- **Ecosystem constraints:** Several other constraints make combating e-fraud challenging for FIs.
  - **Organizational**: Many FIs lack budget and the staff strength needed to implement effective fraud management programs and FDP solutions. For large FIs, implementing robust FDP solutions can cost millions of dollars. Also, many FIs' approach is reactive – they act only after a fraudulent attack has occurred. Consequently, as soon as these FIs address one specific fraud type on a particular channel, it's not too long after that they need to grapple with another fraud type perpetrated elsewhere in their enterprise, via another product or channel.

    Further, in a hypercompetitive environment, FIs willy-nilly succumb to speed-to-market pressures. Many hastily launch new products and services without enabling robust inbuilt anti-fraud capabilities. Customers' unrealistic expectations of frictionless transactions and superlative user experience don't help the FIs' cause either. For FIs, balancing the conflicting needs of their customers' exceptional user experience expectations and that of their fraud management team's security imperatives is always challenging. Many FIs' cybersecurity and fraud management team also find navigating through the myriad cybersecurity standards (e.g. ISO 27001 and 27002, PCI DSS, NERC, NIST, ISO 15408, RFC 2196, ISA/IEC-62443 etc.) confusing.
  - **Regulatory**: Countering fraud and at the same time keeping track of and complying with the fast evolving regulatory landscape is quite a challenge for most FIs. For example, the 'Do-Not-Track' legislation was introduced by the US Federal Trade Commission (FTC) with the goal of safeguarding consumer privacy. However, unintentionally, this legislation also creates fraud management hurdles for FIs. For instance, when such regulations mandate firms to reveal how they utilize the customer information that they collect, it also inadvertently exposes to fraudsters these firms' confidential techniques of discovering frauds. With such knowledge in hand, fraudsters can create myriad new security challenges for FIs.

    As another example, under European Union (EU) Second Payment Services Directive (PSD2), banks need to implement application programming interfaces (APIs) and open up their infrastructure to Third Party Payment Service Providers (TPPs). While this would certainly bring in myriad benefits to the EU payments ecosystem, many security experts also opine that this would create new opportunities for fraudsters. Post PSD2 implementation, it is likely that many customers would no longer need to log onto their banks' websites, and can transact indirectly via the TPPs. Consequently, owing to the lack of direct interactions with their customers, there would be reduction in the amount of relevant customer transaction data available with the bank. This lack of data would adversely impact bank's fraud scoring models that are used for detecting and preventing real time frauds.

    Some of the existing antifraud regulations unwittingly discourage fraud management collaboration between the ecosystem players (issuers, merchants, processors, acquirers, service providers etc.). Instead, these regulations unintentionally force concerned entities to take a 'pass-the-parcel' approach – in which one entity legitimately ends up passing the fraud liability onto another.
  - **Alternative business models**: The explosion of alternative payments providers (such as PayPal, Apple Pay, Skrill, Square, Stripe etc.) have also created challenges for FIs. When these alternative providers link a customer's DDA or card account into their own systems, traditional FIs, unlike earlier, can no longer access and have visibility into some of the customers' transactional information - and which they could have otherwise fed into their fraud scoring models. FIs don't receive highly granular information on transactions executed via these alternative providers. For example, where an issuing bank might have earlier been able to view the location and product purchased information against such transactions, now they may only see "Square" or "Apple" mentioned along with the amount for such transactions. With such partial information, FIs cannot gain complete insights on a customer's financial behavior and purchasing patterns.

Conclusion

It is beyond contention that, more than ever, effective fraud management needs to be a key priority for FIs. After all, today fraudsters' creativity and determination in perpetrating e-frauds is unparalleled. It is therefore imperative that FIs become similarly agile and resolute in combating e-frauds. For this, they need to, with urgency, implement robust fraud management programs and advanced anti-fraud solutions. However, in order to do this, FIs must first gain a deeper understanding of the key challenges that they face in combating the new age e-frauds.

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.rsa.com/content/dam/rsa/PDF/2016/10/2017-global-fraud-forecast-infographic.pdf
- https://nacm.org/pdfs/surveyResults/afp-payments-fraud-results.pdf
- https://www.cifas.org.uk/secure/contentPORT/uploads/documents/Cifas%20Reports/External-Cifas-Fraudscape-2014-online.pdf
- https://www.handbook.fca.org.uk/handbook/document/FC1_FCA_20150427.pdf
- https://www2.deloitte.com/content/dam/Deloitte/in/Documents/finance/in-fa-banking-fraud-survey-noexp.pdf
- http://www.worldpay.com/sites/default/files/Fraud-trends-2016.PDF
- https://www.aciworldwide.com/-/media/files/collateral/trends/preventing-money-laundering-and-bank-fraud-in-the-banking-industry-cs-us.pdf
- https://www.pwc.com/gx/en/financial-services/publications/assets/pwc-gecs-2014-threats-to-the-financial-services-sector.pdf
- https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2016.pdf
- http://www.forbes.com/sites/johnrampton/2015/04/14/how-online-fraud-is-a-growing-trend/#5968b4bd349f
- https://www.datavisor.com/quick-takes/datavisors-predictions-for-2017-thoughts-on-fraud-and-whats-ahead/
- http://www.business2community.com/cybersecurity/payment-trends-2017-fighting-fraud-using-machines-01690864#iKlhof3CwUY6hH75.97
- http://www.aarp.org/money/scams-fraud/info-2016/2017-scams-to-avoid.html
- https://www.internetretailer.com/commentary/2016/10/20/e-commerce-fraud-predictions-2017
- http://www.newindianexpress.com/lifestyle/tech/2016/dec/13/india-to-see-65-rise-in-mobile-frauds-in-2017-study-1548544.html
- https://www.finextra.com/newsarticle/28744/double-headed-beast-swipes-4-million-from-business-bank-accounts
- https://www.finextra.com/newsarticle/30493/financial-sector-breaches-skyrocket-in-2016
- https://securityintelligence.com/shifu-masterful-new-banking-trojan-is-attacking-14-japanese-banks/
- http://www-03.ibm.com/press/us/en/pressrelease/52210.wss
- http://www.itsecurityguru.org/2017/04/03/fico-reports-70-rise-debit-cards-compromised-u-s-atms-merchants-2016/
- http://www.fico.com/en/blogs/fraud-security/hacked-atms-lead-to-70-rise-in-debit-card-fraud/
- https://www.financialfraudaction.org.uk/news/2016/10/12/scams-and-online-attacks-drive-fraud-increase-figures-show/
- http://www.pymnts.com/global-fraud-attack-index/
- https://www.pymnts.com/fraud-attack/2016/fraud-frightening-surge/
- http://blogs.rsa.com/2017-global-fraud-cybercrime-forecast/
- http://www.aol.co.uk/money/2017/03/15/customers-given-anti-scam-tips-as-a-2-million-a-day-is-lost-to-f/
- http://money.cnn.com/2015/03/18/technology/apple-pay-fraud/
- https://www.bba.org.uk/wp-content/uploads/2014/06/BBAJ2110_Cyber_report_May_2014_WEB.pdf
- https://www.washingtonpost.com/business/technology/apple-pays-pitch-simpler-is-better-but-some-security-experts-disagree/2015/03/23/4b22520c-cd7b-11e4-8c54-ffb5ba6f2f69_story.html?utm_term=.beeb4d15dc10
- https://www.fiserv.com/resources/PaymentFraudManager_POV_1507.pdf
- http://www.experian.com/assets/decision-analytics/white-papers/juniper-research-online-payment-fraud-wp-2016.pdf
- https://www.europol.europa.eu/sites/default/files/documents/1public_full_20_sept.pdf

For more information, contact askus@infosys.com

Infosys®
Navigate your next