DISCOVER. SHARE. EVALUATE.

EKN℠

Research Partner

Radial

Trends in e-commerce & digital fraud: Mitigating the risks

Introduction

E-commerce, online, web-connected device (i.e. Internet of Things) related fraud is witnessing an upward trend, with merchants experiencing revenue loss as a result of fraudulent transactions. The Y-o-Y increase in physical POS fraud is 3% compared to a 9-12% increase experienced by e-commerce/ online and mobile merchants. E-commerce, online, web-connected device (i.e. Internet of Things) related fraud is defined as any type of false or illegal transaction, payment or identity-related fraud or personal data theft completed by a cyber-criminal leading to losses in terms of consumer confidence, margin, brand equity, sales, chargebacks or losses incurred by merchants/retailers, suppliers or the financial institution.

How does fraud impact e-commerce businesses?

Direct annual financial loss

Data breaches and jobs

High reputation risks

The effect of fraud on the online merchant or retail e-commerce business can be assessed from three perspectives[1]. Firstly, in terms of direct annual financial loss, companies are losing in excess of $5 million of stolen data. Others have suffered losses that exceed $100 million. Secondly, data breaches and jobs pose a major concern for e-commerce companies. Data breaches have an impact on revenue and job losses. The incidents of data breaches are estimated to harm the global economy to the tune of $2.1 trillion by 2019. In any retail organization, the job of top e-commerce and IT personnel, including CIOs gets jeopardized on account of data hacking[2]. For instance, Katherine Archuleta, the director of the US Office of Personnel Management, had to resign because of data breach. The third major perspective on fraud is related to high reputation risks for the retailer. Whenever a company's security lines are broken, the trust and confidence of e-commerce and mobile shoppers take a hit. Trust and loyalty are crucial for retailers. In order to maintain customer faith, companies must prioritize data security.

[1] https://www.forbes.com/sites/steveolenski/2016/08/03/the-effect-of-cyber-crime-on-online-shopping/#3c7f7d32b873

[2] http://www.informationweek.com/government/cybersecurity/14-security-fails-that-cost-executives-theirjobs/d/d-id/1321279

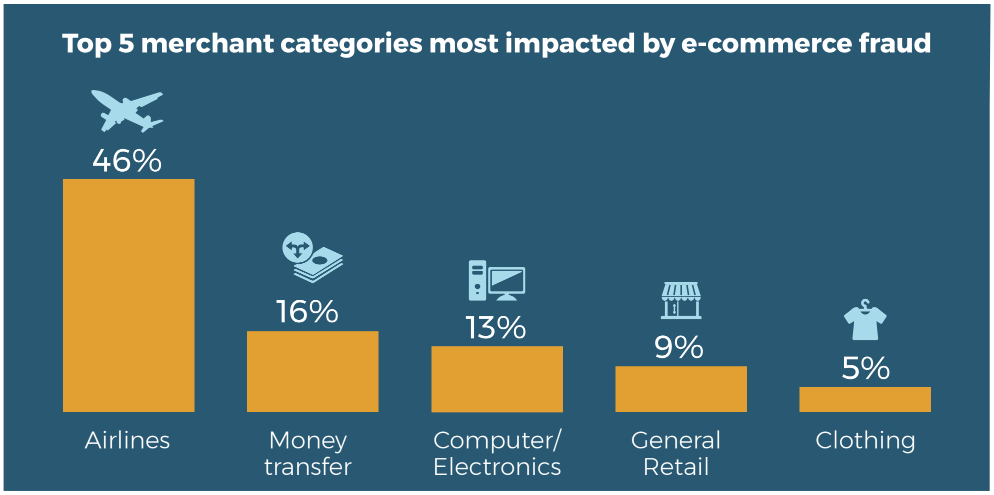
Trends in e-commerce fraud

According to data released by ACI Worldwide, the number of e-commerce fraud attempts based on the total population (i.e., global retailers) increased to 1.49% in 2015 compared to 1.39% in 2014[3]. However, this number increases rapidly during the holiday season. For example, the latest data released by ACI worldwide for the year 2017 reveals that the fraud attempts grew by 31% during Thanksgiving between 2015 and 2016[4].

Fraud attempts are the highest during Christmas eve (2.4%), Thanksgiving (2%), Black Friday (1.8%) and holiday shipment cutoff days (1.6%)[5]. It is also evident that the fraud-related revenue loss doubled between 2014 and 2015. This resulted in retailers losing approximately 1.32% of fraud-related revenue in 2015, up from 0.68% in 2014[6]. Sales via 3rd party websites such as Amazon and eBay are most susceptible to fraud (69%), followed by mobile sales (64%) and retailer owned e-commerce sites (55%)[9]. This indicates that fraud impacts all types of e-commerce and marketplace sites.

The top 5 merchant categories that are most affected by e-commerce fraud are: airlines (46%), money transfer (16%), computer/electronics (13%), general retail (9%), and clothing (5%)[7]. These merchant segments are impacted by fraud incidences that can be categorized into three main categories. The most common type of fraud is identity theft (71%), followed by phishing (66%) and account theft (63%).[10]

In fact, around 40% of e-retailers felt that fraud incidences have been increasing since 2015. 22% felt that fraud incidences have decreased and 40% said it remained the same[8]. The true cost of dealing with online fraud, both within online and offline channels, is growing, with retailers or merchants losing $3.08 for every dollar of fraud they incurred in 2014. This is up


Top 5 merchant categories most impacted by e-commerce fraud

[3] Juniper research, http://www.experian.com/assets/decision-analytics/white-papers/juniper-researchonline-payment-fraud-wp-2016.pdf, http://www.securitymagazine.com/articles/86878-holiday-season-ecommerce-fraud-rates-rise

[4] https://www.aciworldwide.com/news-and-events/press-releases/2017/january/global-fraud-attemptsincreased-by-31-during-holiday-shopping-season

[5] ACI Worldwide

[6] LexisNexis study True Cost of Fraud 2015, http://www.hardwareretailing.com/e-commerce-driving-retailfraud-loss/

[7] Juniper research, http://www.experian.com/assets/decision-analytics/white-papers/juniper-researchonline-payment-fraud-wp-2016.pdf, http://www.securitymagazine.com/articles/86878-holiday-season-ecommerce-fraud-rates-rise

[8] https://www.internetretailer.com/2016/10/28/cost-fraud-76-online-retailers-revenue

[9,10] Worldplay

from $2.79 in 2013. M-commerce-related frauds are driving these costs upward, since the e-commerce fraud cost is higher on mobile platforms than through other forms of payment.[11]

Credit card fraud costs merchants around $190 billion every year[12]. Remote channels[13] have been hit harder by fraud compared to physical store POS. The Y-o-Y increase in physical POS fraud is 3% compared to a 9-12% increase experienced by e-commerce/online and mobile merchants. While EMV transactions prevent fraud losses from occurring at physical store POS, e-commerce fraud has increased. Of all types of thefts, identity theft is posing the biggest challenge for remote channel merchants. In many developed countries, CNP (card not present) represents 60-70% of all card frauds and is increasing every day[14]. CNP frauds drove a 18% increase in overall card frauds in the UK in 2015, the biggest jump in Europe from 2014[15]. The value of fraudulent CNP transactions in Australia rose nearly 25% to AU$402 million ($292 million) in the first six months of 2016, accounting for 77% of all card frauds in that country[16].

EKN's analysis shows that larger merchants with multiple channels are experiencing the highest fraud volume. Mobile channel as a percent of successful fraud transactions among large remote channel merchants has grown Y-o-Y from 26% to 35% (2015-16). If total fraud transactions increase including mobile channel fraud incidence, the share of fraud to total retail revenue also increases. Larger remote channels are also losing out owing to fraud costs, especially mobile and cross-border transactions that experience 15-20% higher fraud costs as a percent of annual revenue than even the average multi-channel merchant.

Mobile channel fraud transactions has grown Y-o-Y from **26% to 35%** (2015-16)

[11] http://www.forbes.com/sites/johnrampton/2015/04/14/how-online-fraud-is-a-growing-trend/#3477fb57349f

[12] http://www.thinksaveretire.com/2015/09/14/how-credit-card-fraud-detection-works/

[13] Remote channels include online, mobile, mail & telephone channels

[14] Juniper research, http://www.experian.com/assets/decision-analytics/white-papers/juniper-researchonline-payment-fraud-wp-2016.pdf

[15] Euromonitor and FICO, https://cardnotpresent.com/cnp-drives-18-card-fraud-increase-in-uk-aug-11-2016/

[16] Australian Payments Clearing Association (APCA), https://cardnotpresent.com/cnp-fraud-surges-25-inaustralia-during-first-half-of-2016/

Methods of payment fraud

The multiple methods of payment fraud[17] include:

- **Phishing:** The fraudulent practice of sending emails purporting to be from reputed retail companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers. Any unfamiliar source is an indication of phishing activities.
- **Identity theft:** The fraudulent practice of using another person's name and personal information in order to obtain credit, loans, etc. A cybercriminal, who steals personal information and uses it under false pretense, is engaging in identity theft. Hackers penetrate firewalls through old security systems or by hijacking login credentials via public Wi-Fi. Many retailers offer Wi-Fi across stores for public access.
- **Pagejacking:** The behavior of stealing high-ranking web page content from another site and placing it on your site in the hope of increasing your own site's search engine rankings. Hackers can reroute traffic from a retailer's ecommerce site by hijacking part of it and directing visitors to a different website. The unwanted site may contain potentially malicious material that hackers use to infiltrate a network security system.
- **Advanced fee and wire transfer scams:** Hackers target credit card users and ecommerce store owners by asking for money in advance in return for a credit card or money at a later date.
- **Merchant identity fraud:** This method involves criminals setting up a merchant or retailer account as if it is a legitimate business and charging stolen credit cards. The hackers then vanish before the cardholders discover the fraudulent payments and reverse the transactions. When this happens, the payment facilitator is liable for the loss and any additional fees associated with credit card chargebacks.

Decoding the methods of online or e-commerce fraud

Individuals or groups indulging in fraudulent e-commerce and m-commerce transactions apply varied methods including unauthorized account access, card usage, among other fraud techniques. Some of these major fraud methods are outlined below:

- **Account Takeover (ATO)[18]:** Unauthorized access and control of another user's personal information online is the most prevalent type of fraud in the e-commerce domain. Around 40% of e-commerce fraud falls under the ATO variety. ATO – also known as identity theft – occurs when one user obtains the credentials to another user's value storing account. A value storing account can be anything from a bank account to a gaming account to a Facebook profile. According to Javelin Strategy & Research, ATO takes place every three seconds in the US.

[17] https://www.bigcommerce.com/ecommerce-answers/payment-fraud-what-it-and-how-it-can-be-avoided/

[18,19] https://www.2checkout.com/upload/documents/ebook_Guide_to_Ecommerce_Fraud.pdf 19 https://www.2checkout.com/upload/documents/ebook_Guide_to_Ecommerce_Fraud.pdf

- **Credit Card**[19]**:** A stolen credit card can be used for extensive fraud. CNP (Card Not Present) credit card fraud constitutes any illegitimate buying and selling transaction that takes place online with stolen credit information: it can involve sales, resales, or returns. There are 2 subtypes of credit card fraud:
    - **Friendly fraud:** Known as the more explanatory "chargeback fraud," a "friendly" fraud occurs when a customer makes an online purchase with his or her own credit card and then requests a chargeback (money returned from the transaction for an alleged fault in the product) from the bank or credit card company after receiving the item or service.
    - **Triangulation scheme:** In this type of fraud, the fraudster purchases an expensive item from one e-commerce domain (using a stolen card or employing deliberate friendly fraud) and visits a second website (a seller's website that accepts public merchants, such as eBay) and sells the item to a third unsuspecting individual. The faster the transactions occur, the less time either website has to conduct the appropriate checks and balances to determine the validity of the card, which may be stolen. The fraudulent party is paid by the third party, while the original merchant has either accepted payment from a stolen credit card (which will result in a chargeback) or suffers a chargeback as the fraudster claims that he or she never received the merchandise.
- **Malware:** Malware is a malicious software such as trojans and viruses, designed to infect your computer without your informed consent or knowledge. It can monitor your keystrokes (thereby recording everything you do), take control of your computer, or do any number of other things that can affect the performance of your computer. Malware is generally distributed through email, social networking sites and video sites[20].

The financial impact of online or e-commerce fraud

E-retailers spend more than 7% of their annual revenue to deal with fraud[21]. Digital goods merchants suffered the worst losses, at 8.6% of revenue on an average, but hybrid goods merchants faced similar costs at 8.1% of revenue. Data shows that fraud and chargeback management can consume between 14% and 23% of the operational budget.

Large e-commerce merchants or retailers lost 1.39% of revenue to fraud on an average in 2015, despite spending around $115,000 annually on fraud mitigation. However, it is the mobile commerce and international merchants that reported the highest fraud losses at 1.68% and 1.58%, respectively[22].

According to EKN analysis, the cost of fraud includes replacement of goods, shipping & insurance costs, manual review costs, chargebacks, investment and operational costs involving fraud detection and prevention solutions. If all of the above costs are included, LexisNexis estimated that the true or total cost of fraud for online merchants in 2015 was $223 for every $100 of goods lost.

[20] http://www.tescobank.com/security/how-fraud-occurs/)

[21] The Financial Impact of Fraud: Merchants Challenged As E-Commerce Fraud Rises Post-EMV, https:// www.internetretailer.com/2016/10/28/cost-fraud-76-online-retailers-revenue. The first 4 data points is taken from the same link

[22] Juniper research, http://www.experian.com/assets/decision-analytics/white-papers/juniper-researchonline-payment-fraud-wp-2016.pdf

How well are retailers tackling online or e-commerce fraud issues?[23]

A manual review of fraud is next to impossible due to the sheer volume of commerce managed by online retailers. Consequently, there is a need to imbibe a system that can flag suspicious transactions across various retail channels. 66% of retailers use fraud mitigation solution compared to 30% of retailers, who use an automated flagging system. However, for large e-commerce/m-commerce retailers, more than 80% use a fraud mitigation solution and on an average, such merchants use 5–6 fraud mitigation solutions.

66% of retailers use fraud mitigation solution compared to **30%** of retailers, who use an automated flagging system

Meanwhile, the larger remote/international channel merchants are more likely to track fraud costs by the payment method, while tracking fraudulent transactions by channel. International retailers or merchants spend a significant amount of time and resources on manual reviews. While large remote channel merchants spend nearly half of their mitigation budgets on solutions, they have a sizeable portion that is allocated to manual reviews and physical security. In a complex omnichannel scenario, this adds to the cost of fraud mitigation. Excessive manual reviews pose a problem for e-commerce companies engaged in cross-border selling. There is concern among both large e-commerce/ m-commerce merchants about the new and varied payment methods in diverse international settings, where each country and region has its own laws, taxation rules and customs. Merchants do not feel as if they have the right specialized tools to manage cross-border e-commerce fraud.

Large m-commerce merchants, have concerns about identity verification once its transactions cross the border (44% selling internationally versus 30% domestic). Moreover, among these large m-commerce merchants, there is little consensus around which solutions are most effective for controlling fraud internationally. While solutions have emerged for domestic fraud management, they are not suitable for remote channels and can be tricked by fraudsters. Off-late, remote channel merchants have started investing in multiple solutions involving a multilayered approach of advanced identity and transaction verification/authentication to realize lower false positive rates than others.

[23] The entire section has been referred from the following: http://images.solutions.lexisnexis.com/Web/LexisNexis/%7Bea78e9df-056e-46ed-b04c-e8bfbc526ffd%7D_2016_True_Cost_of_Fraud_Study_052516. pdf?elqTrackId=cc6d22e0b40d4a29a2931f28fb221092&elqaid=2567&elqat=2

Process and knowledge capabilities that can be used to avoid online or e-commerce fraud

Modern e-commerce fraud prevention capabilities[24]

- **PCI-DSS:** Complying with Payment Card Industry Data Security Standards (PCIDSS) ensures that your systems are secure, customers can trust you with sensitive data, and it improves a retailer's reputation. To be awarded this certification retailers or merchants are required to utilize advanced fraud and risk management technology with the latest algorithms for fraud checks. Retailers or merchants must enact stringent security procedures and meet the strict standards set by the PCI DSS. Working with a payment processor that is PCI DSS certified, such as 3G Direct Pay, can reduce the cost and burden of maintaining PCI compliance certification for merchants, themselves.
- **AVS:** Address Verification System is an automated fraud prevention method used to reduce the risk for merchants selling in the "card not-present" environment (e. g. online or telephone purchase). AVS checks the billing address listed in the transaction against any other address registered with the issuing bank. Retailers or merchants should request both billing and shipping addresses of the consumer so that an AVS check can be conducted before a transaction is processed.
- **CVV:** Card Verification Value is a three-digit security code printed on the back of the credit or debit card (in the case of American Express, four digits on the card front). It is not stored in the magnetic strip or embossed on the card, so it cannot be easily retrieved by thieves unless the card is in their possession. Visa calls it a CVV2, MasterCard calls it a CVC2, and American Express calls it CID.
- **Geolocation by IP address:** This can help identify a consumer's precise location or determine the distance between the billing address of the person, who is paying for the product, and actual location of the perso,n who is placing the online order. Thus, it acts as an additional verification measure or authentication for transactions that have significant discrepancies. Geolocation technology provides information that enables online business owners conclude which transactions to look deeply into and which to clear. This leads to a balance between the risks of losses due to fraudulent activity and the risk of preventing legitimate customers from completing their purchases.
- **Anonymous proxy server:** Anonymous proxy servers enable people to hide their real IP addresses. Proxy servers are used by fraudsters as they help them stay anonymous and avoid detection. Detecting an anonymous proxy server is no simple task, as they appear and disappear sporadically.
- **Compare the IP address country with the billing address country:** Check whether the IP address of the customer and the billing address belong to the same country where the product will be delivered. If a customer's shipping and billing addresses are in Canada, but the order was placed from an IP in Ukraine, one should closely scrutinize the transaction.

[24] The first 8 points have been referred from the following: http://www.directpay.online/blog/understanding-online-fraud-and-how-to-mitigate-the-risks-part-2/

- **Security services:** Using a "trust mark" security service that scans your systems daily to search for malware and vulnerabilities is a superb tactic for reducing fraud as it adds an additional level of security. In addition to your own fraud prevention measures, and those of your payment processor, a security service gives the added protection to make your online business even safer. TRUSTe, Verisgn, or McAfee Secure are examples of services that help avoid and catch problems fast. They also increase customer trust and decrease the attractiveness of your site to hackers.
- **3D secure:** Implementing 3D Secure offers merchants an additional security layer for online credit and debit card transactions. This goes a step further than standard comprehensive fraud protection, as it ties the payment authorization process to an additional online authentication step in which the end user is prompted to enter a password known only to the bank and the customer. Visa offers 3D Secure as Verified by Visa, MasterCard as MasterCard SecureCode; JCB International as J/Secure and American Express as American Express SafeKey in select markets.
- **Layer IP intelligence data**[25]**:** Layering in domain, ISP, proxy, and hosting center data allows the identification of more suspicious connections. Merchants or retailers should be cautious when selecting an IP intelligence solution. There is a big difference between premium IP intelligence providers, who deploy multiple methodologies to analyze IP routing infrastructure, and those who simply repackage outdated and patchy publicly available data.

[25] http://news.retailrisk.com/news/five-steps-to-substantially-reduce-online-payment-fraud-using-ip-intelligence/

Use of technology to prevent e-commerce fraud

- **Enabling secure login credentials for customers:** Accepting payments through customer login and eliminating using checkout through a guest profile can help reduce fraud incidence. Purchasers must be able to securely log in with their own credentials. This can aid in behavioral analytics to sift out "questionable" accounts and ensure that bad actors are shut down before they do damage[26].
- **Use of 3D secure protocol:** EMV will undoubtedly continue to push fraud to the CNP (Card Not Present) channel where there is low hanging fruit for bad actors. Combining a comprehensive fraud prevention strategy with the 3D secure tools offered by the card brands can ensure retailers or merchants are on the right side of the liability shift for authenticated transactions and reduce costs associated with manual reviews and interchange rates[27].
- **Combine machine learning with human intervention:** Advanced machine learning will take the driver's seat as datasets grow bigger. As a result, it has become exceedingly difficult for companies to effectively analyze this information and draw conclusions. While advanced machine learning automates these tasks to make the process more effective and less time-consuming, human intervention or manual fraud data review capabilities is required for interpreting fraud data in the context of how fraud has impacted the e-commerce business and customer experience. This technology will be important to many different important business issues, but fraud prevention will be one of the biggest applications, especially in light of other security and fraud prevention trends moving into the new year. Tracking omnichannel customers and keeping an eye on data from social media and the Internet of Things (IoT) will require enhanced security technology[28].
- **New fraud detection tools:** A handful of security vendors have responded to the increasing threat of online or e-commerce fraud by developing new fraud detection tools and advanced MFA (multi-factor authentication) techniques, involving OOB (Out-of-Band) authentication and using biometric technology for identity verification.

However, there is a flip side to use of technology[29]

Emerging payments technology and the IoT will increase security risks. Smart devices, wearables and the evolution of the Internet of Things effectively means more personally identifiable information (PII) will be circulating. Given the already difficult job of providing secure and sensitive information merchants or retailers face, these new technologies will further complicate matters.

[26, 27] http://www.verifi.com/in-the-news/what-do-i-need-to-know-about-online-payments-fraud-in-2016/

[28] http://feedzai.com/blog/5-fraud-prevention-trends-for-2016/

[29] http://www.verifi.com/in-the-news/what-do-i-need-to-know-about-online-payments-fraud-in-2016/

Recommendations

Invest in Top-of the-Range FDP (fraud detection and prevention) Solutions:

- Offer real time as well as cross-channel monitoring of all transactions.
- Consider solutions that offer machine learning and algorithm-based solutions that can analyze large swaths of data and can also handle human/manual data interpretation when needed.

Implement mobile security measures:

- Accelerate use of key smartphone sensors such as accelerometers, cameras, GPS receiver, microphone and fingerprint/iris sensors to provide advanced biometric security.
- E-commerce, financial services and consumer electronics biggies such as MasterCard, Visa, Google, Samsung and Microsoft, have already started using biometric-authentication as a replacement for passwords, thus following in the footsteps of Apple that unveiled biometric identification in its smartphone products since 2013.

Initiate cross-industry collaboration:

- Existing legislation promotes ‘pass the parcel approach’ rather than a collaborative approach.

Our research agenda is developed using inputs from the end user community and the end user community extensively reviews the research before it is published. This ensures that we inject a healthy dose of pragmatism into the research and recommendations. This includes input of what research topics to pursue, incorporating heavy practitioner input – via interviews etc., and ensuring that the blend of research takeaways are oriented toward a real-world, practical application of insights with community sign-off. For more information, visit **www.eknresearch.com**.

Radial is the leader in omnichannel commerce technology and operations, enabling brands and retailers to profitably exceed retail customer expectations. Radial's technical, powerful omnichannel solutions connect supply and demand through efficient fulfillment and transportation options, intelligent fraud, payments, and tax systems and personalized customer care services. Hundreds of retailers and brands confidently partner with Radial to simplify their post-click commerce and improve their customer experiences. Radial brings flexibility and scalability to their supply chains and optimizes how, when and where orders go from desire to delivery. Learn how we work with you at **www.radial.com**.

Disclaimer: EKN does not make any warranties, express or implied, including, without limitation, those of merchantability and fitness for a particular purpose. The information and opinions in research reports constitute judgments as at the date indicated and are subject to change without notice. The information provided is not intended as financial or investment advice and should not be relied upon as such. The information is not a substitute for independent professional advice before making any investment decisions.

Registered Office: 570 Lake Cook Road, Suite 310, Deerfield, IL 60015 | Ph: (973) 607-1300