Understanding the True Costs of Fraud

Version 1.0

Publication Date: November 2018

U.S. Payments Forum
191 Clarksville Road
Princeton Junction, NJ 08550

www.uspaymentsforum.org

About the U.S. Payments Forum

The U.S. Payments Forum, formerly the EMV Migration Forum, is a cross-industry body focused on supporting the introduction and implementation of EMV chip and other new and emerging technologies that protect the security of and enhance opportunities for payment transactions within the United States. The Forum is the only non-profit organization whose membership includes the entire payments ecosystem, ensuring that all stakeholders have the opportunity to coordinate, cooperate on, and have a voice in the future of the U.S. payments industry. Additional information can be found at http://www.uspaymentsforum.org.

EMV is a trademark owned by EMVCo LLC.

Table of Contents

1. Background

Some 15.4 million consumers were victims of identity theft or fraud in 2016, according to a report from Javelin Strategy & Research. That's up 16 percent from 2015, and the highest figure recorded since the firm began tracking fraud instances in 2004.[1]

According to numbers released by the Identity Theft Resource Center (ITRC) and CyberScout, the number of U.S. data breaches tracked through June 30, 2017 hit a half-year record high of 791 – almost 30 percent higher than the same period in the previous year.[2]

The Nilson Report, a publication covering global payment systems, reported that global card fraud losses equaled $22.80 billion in 2016, an increase of 4.4 percent over 2015. Card issuers incurred 70.7% and merchants, their acquirers and ATM acquirers incurred 29.3% of those losses.[3] These amounts do not include costs incurred by retailers, card issuers, and acquirers for their operations and chargeback management.

The 2018 LexisNexis® The True Cost of Fraud Study stated that U.S. merchants' impact of fraud losses as a percentage of revenues has moved upwards from 2017 to 2018 (1.58% to 1.80% on average) This 13.9% increase is up from 8% the previous year.[4]

With the rollout of EMV in the United States, card issuers and merchants invested vast amounts of money to reduce their respective institutions potential fraud losses resulting from counterfeit magnetic stripe fraud. The natural assumption is a seismic shift would be experienced with card-not-present channels being saturated with fraudulent attacks. As fraudsters modify their attacks and find new channels for fraud, all who participate in the payment ecosystem must remain adept and continue to adapt. All stakeholders – customers, vendors, financial institutions, and everyone in between – are impacted in a variety of sometimes underappreciated ways.[5]

The objective of this white paper is to highlight the myriad forms these impacts take and the impact they have on the various stakeholders, providing insights from different perspectives. The white paper presents three example case studies from different stakeholder perspectives to illustrate the cost of fraud. The consumer, card issuer and merchant were selected to highlight as stakeholders because they experience the most pain points in mitigating fraud risk and most measurable losses when calculating the cost of fraud.

Electronic commerce relies on a network of solutions and suppliers which together enable transactions, both legitimate and fraudulent. The complexity will vary depending on factors including size, type of merchant, history, location, risk, and types of payment cards. As one scenario is insufficient to provide useful perspectives of the impact of fraud, three points of view have been selected for this white paper — and each is presented with a specific story to focus the discussion of the related costs.

The reference to the "true cost of fraud" in the white paper title reflects the fact that the costs associated with fraud extend beyond monetary value and also include reputational, operational, and

---

1 https://www.cnbc.com/2017/02/01/consumers-lost-more-than-16b-to-fraud-and-identity-theft-last-year.html

2 http://www.idtheftcenter.org/Press-Releases/2017-mid-year-data-breach-report-press-release

3 Source: Nilson Report, October 2017

4 https://risk.lexisnexis.com/insights-resources/research/2018-true-cost-of-fraud-study-for-the-retail-sector

5 Various methods are used by stakeholders to mitigate card-not-present fraud. See the U.S. Payments Forum white paper, "Near-Term Solutions to Address the Growing Threat of Card-Not-Present Fraud," for a discussion on mitigation approaches, available at http://www.emv-connection.com/near-term-solutions-to-address-the-growing-threat-of-card-not-present-fraud/.

regulatory costs. A table is included with each of the three case studies listing the descriptions of cost for the use case participant. The table includes columns indicating both "hard costs" and "soft costs."

- Hard costs are discrete, measurable expenses. Examples are: a consumer's loss of goods and/or services; a financial institution's loss in spend; and a merchant's loss of sales.
- Soft costs are expenses whose impact is difficult to measure. Soft costs could include, but are not limited to: reputational impacts for the consumer; and operational and regulatory impacts for the financial institution and merchant.

This paper does not include monetary values. The focus of the white paper was to identify the types of cost and to present these in high-level, logical groupings. This approach allows readers to understand the overall fraud scenarios and then apply specific conditions and values that are relevant for their own use.

Intended Readers

This white paper was created for financial institutions, merchants, vendors, or other interested parties or stakeholders that have an interest in understanding the complexities and costs associated with the true cost of fraud. Interested parties could include, but are not limited to, product managers, business analysts, finance managers, program managers, and those involved in operational support areas including card issuance and fraud management.

The perspectives provided in this paper are based on the knowledge and expertise of the participating U.S. Payments Forum members and may be limited in scope. Fraud and fraud mitigation strategies continue to evolve; this white paper represents a snapshot of experiences resulting from fraud from the perspectives of three different stakeholders in the ecosystem.

The information is intended to be informational. Organizations should assess their own situations and consider their risk tolerance and their approach to managing fraud cost.

Additional Supporting Materials about Fraud from the U.S. Payments Forum

Fraud trends and mitigation approaches are important topics for the U.S. Payments Forum. The Card-Not-Present Fraud Working Committee has published several white papers and plans to continue development of materials to support the payments industry in the fight against CNP fraud.

Refer to the U.S. Payments Forum website for the latest materials, including fraud mitigation best practices and solutions plus evolving fraud trends: http://www.uspaymentsforum.org/working-committees-sigs/card-not-present-fraud-working-committee/.

2. Consumer Case Study

Robert is an active shopper with several payment cards from different financial institutions. Like many consumers, Robert's choice in how he pays is often influenced by the rewards that are available with a specific card. He uses three different credit card accounts regularly – one for his frequent online shopping activity, another account for travel and restaurants, and yet another for large purchases on which he carries a balance. He also uses his debit card for gasoline and grocery purchases.

Robert uses credit responsibly, has never been delinquent on an account, and has never had a late payment. While Robert does not check his credit scores regularly, he recalls that his score was in the very good to excellent range when last checked.

Robert has started shopping for his first home and is looking to get pre-approved for a home loan. In reviewing his application results and credit reports, Robert is startled to see that his credit score is almost 250 points lower than expected, and his credit report shows a number of credit card accounts that he did not open. Based on the information on the credit report, it appears that the unfamiliar accounts were all opened within the same two-month period in the previous year; each account was used regularly for several months and minimum payments were made, all on time. The fraudster then made a series of larger online purchases and abruptly abandoned the accounts. All of the new accounts were now delinquent, and some have been forwarded to collection agencies. Upon investigation, Robert realized that the fraudsters obtained his credentials from a data breach.

Robert now faces the daunting task of repairing his credit history.

- Robert will need to document the crime and report it to law enforcement. Depending on local resources available, this could result in many hours of work on his part.
- He will have to find the appropriate contacts at the lending institutions and work with them – not just those with whom the fraudulent accounts were opened, but also the ones with his valid accounts and those mortgage lenders with whom he applied. Robert will also have to work with the credit reporting agencies and possibly the data collection companies.
- Robert may not be able to qualify for the home loan. In the event that he does qualify, the rates offered may be significantly higher than ones if there hadn't been fraud. Depending on the amount borrowed, higher rates may result in monthly payments that are hundreds of dollars higher.
- Had Robert been looking for employment, he could have had more problems; many companies Include credit checks as part of their onboarding process.

Table 1 summarizes example consumer costs caused by this credit card/identity theft scenario.

Description	Hard Cost	Soft Cost
Physical Cost for Consumer		
Lost wages	X	
Higher interest rates	X	
Value of disputed item (timeline for reporting different for credit vs. debit)	X	
Immediate impact to funds available in account	X	
Possible overdraft fees	X	
Possible returned check fees	X	
Customer Inconvenience Cost		
Time spend with law enforcement		X
Time spent with creditors		X
Reputational Loss Cost		
Credit worthiness		X
Possible lost employment opportunities		X

Table 1. Examples of Consumer Costs Resulting from Credit Card/Identity Theft Scenario

NOTE: Table 1 represents consumer costs typically incurred in an identity theft scenario resulting in credit card fraud. In a debit card scenario, there may be additional costs, including but not limited to possible overdrafts, returned checks due to insufficient funds, fees, and immediate reduction in available account funds.

Statistics indicate that less sophisticated fraud methods, especially card skimming (used to create counterfeit magnetic stripe cards or used to purchase goods online), are more common causes of consumer fraud than the identity theft scenario presented in the case study.

Additional Information

The Federal Trade Commission (FTC) website at https://www.consumer.ftc.gov/features/feature-0014-identity-theft provides substantial information about the impact of consumer identity theft.

3. Financial Institution (Issuer) Case Study

Michael is a premier account holder with a national bank. He has several other accounts with the same bank, including a savings account and a checking account into which his paycheck is deposited regularly. He has no history of fraud reports.

While paying at his local home improvement store, Michael inserts his credit card into the terminal as usual and is surprised when the transaction is declined. The cashier asks Michael if he would like to try the card again or if he would prefer to use a different card. Glancing at the line growing behind him, Michael ignores the faint chimes of an incoming text and email on his phone and hands the cashier another card issued by a different bank. The transaction is then completed without further incident.

Michael returns home and logs onto his online banking application. He notices several transactions at multiple online merchants he does not recognize. He immediately calls the bank's toll-free number and is assisted by Becky, the bank's customer call center representative. With Becky's help, Michael identifies 10 different suspicious transactions, totaling over $5000, occurring on various days over the last week.

Becky flags the unrecognized activity for further investigation and dispute resolution. She then informs Michael that, for his security, a new card with a new account number will be issued. She will also issue temporary credits to his account while his case is investigated. As part of the bank's processes, Michael will be required to sign an affidavit to affirm the fraudulent charges and return the completed form to the bank. His replacement card will be mailed immediately. Both the affidavit request and the replacement card will be sent to the address on file for the account and should arrive within five business days.

Michael requests that the replacement card be sent to another location overnight, since he is about to leave town on a business trip and had planned to use this card for his expenses.

The next evening Michael arrives at his hotel. After checking in, the hotel clerk hands him a package that had arrived earlier that afternoon via overnight courier. Michael activates his new card.

The scenario described – unfortunately becoming all too common – impacts the bank that issued Michael's declined card in several ways.

- Since Michael eventually used a different card for the transaction at the home improvement store, the bank lost the revenue associated with that particular transaction. Depending on the total amount of the purchase and the number of purchases that were made with the alternative card, this amount can be significant.
- If Michael decides that he no longer wishes to use that account, the incentives the bank provided to Initially acquire Michael's account have been lost as well. These incentives are often made possible through future revenues associated with transactions that are expected to offset the customer acquisition cost. Depending on the incentives provided – miles, points, or statement credits – these costs can be significant.
- The fact that Michael's card was replaced means that the bank incurs the re-issuance costs. The issuer's card replacement costs will depend on the card technology (e.g., traditional magnetic stripe or EMV chip; plastic, graphite or metallic card; powered or display card) and on card delivery costs. Notification letters, inserts, and envelopes to mail the replacement cards result in incremental costs for the bank.
- Michael's request for the replacement card to be sent to a different location means that additional

validation is also required, and other special arrangements made. The costs for delivery via an overnight courier significantly increase the delivery cost above the usual first-class mail option.

- Michael's actual interaction with the call center requires significant bank investment. The interaction Is not limited to the interaction with Becky. Michael will also have used the bank's toll-free number, and he may have had to interact with some sort of automated interactive voice recognition (IVR) system that routes calls to the correct department.
- The type of card, and the features supported by the card, may require that personal identification numbers (PINs) be established. If so, a separate process to provide the PINs will also be necessary.
- Once Michael receives his replacement card, he needs to activate it for use. At least one card activation process (more likely several) must be in place for the issuer. Activation may be done with an automated IVR system, a call center, an online banking web site, or a mobile app, or at a bank branch or ATM. Any combination of these options to support cards replaced due to fraud increases the replacement costs for the bank.

Table 2 summarizes example issuer costs resulting from card fraud.

Description	Hard Cost	Soft Cost
Physical Cost		
Card production and delivery	X	
Loss in spend	X	
Dispute resolution	X	
Operational Cost		
Customer service call center support	X	
Fraud operational support staff	X	
Fraud data analysis – internal or outsourced	X	
Investigation tools and services	X	
Correspondence management	X	
Fraud mitigation tools	X	
Training and awareness	X	
Legal/compliance resources	X	
Customer Inconvenience Cost		
Time without a card		X
Cardholder experience resulting from false positives		X
Reputational Loss Cost		
Wallet position		X
Public perception of a third-party breach		X

Table 2. Examples of Issuer Costs Resulting from Card Fraud

4. Merchant Case Study

Carmen is a fraud agent at ABC Markets, a company with a large store base as well as a thriving ecommerce business. While reviewing online orders, she sees an order for a video gaming system placed on Jason's credit card. The card verification code was entered correctly, but Carmen notices that the address verification system (AVS) response from the credit card authorization indicates that the billing address provided is incorrect. Because gaming system purchases are higher risk than many items ABC sells, she decides to research the transaction further before approving it. The IP address used to place the order is not specific; there are many orders from various customers placed on the same IP. An email data service used by ABC indicates the email address used for the order was created recently but does not have any fraud associated with it. Before making a final decision, she tries the phone number given with the order and it goes directly to voicemail.

It is two weeks before Christmas and the gaming system just went on sale. She knows that sales are going to be strong for this item and that some customers prefer to keep their information relatively private when shopping. Many customers shopping during the holiday season are rushed and don't fill in their information accurately. She wants to make sure she doesn't cancel an order for a good customer, since stock is limited and there might not be any systems left if Jason's order is cancelled and he needs to place a new order. Carmen recalls that her team has not seen any fraud for gaming systems and this type of data mismatch and approves the order. The order is shipped the same day.

A few days later, Jason logs into his online banking website and sees a charge for an ecommerce transaction from ABC. He promptly files an online dispute since he did not make this purchase. His bank files a fraud chargeback for the transaction, which ABC receives from their merchant processor. The team that responds to chargebacks sends the transaction information to the processor; however, since the AVS response was not a match, they are unable to get the chargeback reversed.

This scenario impacts the merchant in several ways:

- ABC receives a chargeback for the full amount of the order since the transaction was not authorized by Jason. This amount is written off to fraud sales expense or chargeback expense.
- Jason was an infrequent shopper at ABC, but after seeing the unauthorized charge on his credit card bill, he places part of the blame on ABC and stops shopping there altogether. It isn't until much later that he learns that his card data was stolen during a breach at another website that he uses for professional networking and realizes that ABC wasn't at fault.
- ABC employs fraud agents, data analysts and customer service representatives to help fight fraud. They also pay for every transaction to go through a fraud screening model housed in a software program that they purchased for fraud management. They also pay for data verification services to assess the risk of a particular computer or phone being used for shopping, and to check an email address for fraud history.
- The order needs to be flagged as fraud, so data can be used for future upgrades to the fraud scoring rules.
- ABC's fraud department needs to ensure all agents are now aware of this fraudulent order, since it may be the start of a new fraudulent order pattern. Most ecommerce fraud comes from organized groups who use identifiable patterns.

This scenario is common for a larger merchant with an in-house fraud team that uses analytics tools and solutions designed specifically for fraud detection and prevention. The expertise and technology that a

merchant has will depend on the merchant size and sales volume, fraud pressure (total attempted fraud) and merchandise assortment. Some may use advanced data tools such as device fingerprinting, user behavioral or web analytics, or payment authentication such as 3-D Secure.

Table 3 summarizes example merchant costs resulting from ecommerce fraud.

Description	Hard Cost	Soft Cost
Physical Cost		
Loss of physical goods	X	
Loss of income for digital goods	X	
Chargebacks	X	
Operational Cost		
Fraud department operations staffing	X	
Fraud data analysis – internal or outsourced	X	
Investigation tools	X	
Data services	X	
Fraud solution software/services	X	
Payment team and services	X	
Customer service call center support	X	
Security/compliance resources	X	
Customer Inconvenience Cost		
Inventory unavailable		X
Decreased shopping due to good customer insult (cancelled-in-error)		X
Increased friction for good guests due to fraud controls		X
Reputational Loss Cost		
Stock price		X
Public perception of a breach		X

Table 3. Examples of Merchant Costs Resulting from Ecommerce Fraud

5. Conclusion

The costs associated with payment fraud extend beyond monetary value and include reputational, operational and regulatory costs. This white paper summarizes three scenarios, providing consumer, issuer and merchant perspectives on "real life" situations and costs. Each section concludes with a table listing examples of costs including both hard and soft costs.

The white paper does not include the actual monetary values of costs resulting from fraud, but rather focuses on identifying the types of cost. The white paper includes links for additional information available from the U.S. Payments Forum website including: CNP fraud trends and mitigation approaches. Readers are invited to consider applicable conditions and values for their own use.

While the white paper doesn't cover the return on investment for fraud solutions and risk mitigation practices, it is important for the reader to keep in mind that substantial investments are made by all payments stakeholders to mitigate fraud.

6. Legal Notice

This information does not constitute legal advice and should not be relied on for any legal purpose, whether statutory, regulatory, contractual or otherwise. All warranties of any kind are disclaimed, including all warranties relating to or arising in connection with the use of or reliance on the information set forth herein. Any person that uses or otherwise relies in any manner on the information set forth herein does so at his or her sole risk.

Without limiting the foregoing, it is important to note that the information provided in this document is limited to the payment networks and other sources specifically identified, and that applicable rules, processing, liability and/or results may be impacted by specific facts or circumstances.

Additionally, each payment network determines its own rules, requirements, policies and procedures, all of which are subject to change.

Merchants, issuers, acquirers, processors and others implementing EMV chip technology in the U.S. are therefore strongly encouraged to consult with all applicable stakeholders regarding applicable rules, requirements, policies and procedures for transaction receipts, including but not limited to their respective payment networks, testing and certification entities, and state and local requirements.