How Merchants & Issuers Can Fight Credit Card Fraud Together: Creating Order with the Right Information and Collaboration

VERIFI™

The premise of this paper is simple: chargebacks and fraud hurt profitability. To add insult to injury, many of these chargebacks are preventable. This is an obvious truth that is grounded in an often not-so-apparent reality: there are very limited mechanisms for merchants and issuers to collaborate and share timely and detailed information that could better pinpoint fraud and help stop disputes from unnecessarily escalating to costly chargebacks.

Chargebacks and fraud increase operational costs for both merchants and issuers, lead to penalties by the card brands and hurt brand reputation and customer retention. Many of these problems could be prevented through simple and more informed exchange of information between merchants, issuers and cardholders. The ability to reduce cardholder confusion or better substantiate legitimate sales can go a long way in stopping friendly and credit card fraud, helping both parties streamline operations and reduce costs, as well as improve customer satisfaction and retention.

As retail and the CNP landscape continue to evolve, both increased regulation and dynamic fraudsters will cause the online channel to become a prime target for fraud and chargebacks. This paper outlines the stark reality of CNP and friendly fraud in the U.S., examines the root of the fraud and chargeback problem and outlines a number of solutions for merchants and issuers to stop unnecessary chargebacks, retain more revenue and protect the bottom line.

The CNP Fraud Reality

Last year, the U.S. carried 47 percent of the world's credit card fraud, even though it owns only 24 percent of the total global volume.[1] As other market factors contribute to growing credit card fraud, U.S. merchants will continue to see a negative impact to their bottom line.

Last year, the U.S. carried 47% of the world's credit card fraud,

even though it owns only 24% of the total global volume.[1]

EMV has been a catalyst to the online fraud boom, and many merchants are still struggling to adapt. One just needs to look abroad to see the potential negative impact to the CNP channel by EMV adoption. It tended to push fraudsters online, marking a sharp increase in CNP fraud. The U.K., for example, had a 360+ percent increase after EMV implementation.[2] Since EMV adoption has been lagging, it's possible that the criminals are lagging in their move online as well. But that doesn't mean merchants shouldn't be preparing.

Despite the slow adoption, it appears that many fraudsters are trying to stay ahead of the curve. A recent Forrester report indicated that fraud losses would rise 55 percent by 2018 in North America.[3] Instances of fraud were up a whopping 163 percent in the first three quarters of 2015 alone.[4] And fraudsters have the upper hand over merchants in other areas as well. They are not encumbered with regulatory or compliance requirements, and they can operate as autonomous agents or groups that work fluidly and with agility.[5]

Emerging Technology Provides Merchants with Both a Blessing and a Curse

While technology like point-to-point encryption or "P2PE" and tokenization aim to combat fraud by encrypting data and payment credentials, fraudsters are proving that they can maintain pace with security technology and, in some cases, beat it. Near the end of 2015, botnet attacks accounted for 82 percent of all fraud attacks in the U.S.[6] In many cases, it's the merchant struggling to keep up with the agility of the fraudster, who seems to have unlimited speed and sophistication while merchants are forced to operate under heavily regulated conditions with limited resources. Until recently, there was no viable alternative, but cutting-edge technology means that's no longer the case. Full automation based on machine learning that adapts with every single transaction is now possible.[7]

Chris Marchand, Vice President of Business Development for Verifi, notes the unique vulnerabilities merchants face with quickly advancing technology:

> "The more advanced technology becomes, it essentially creates more and more ways for a consumer to purchase an item from a merchant, and thus, more access points into the merchant/consumer that need to be secured. Hackers have more channels available to them to capture cardholder data and commit fraud. Consumers and merchants both want less friction during the checkout and purchase process, but this unfortunately comes at a high price. Between mobile payments, Twitter buy buttons, pay by car, pay by Alexa, there are so many more channels to secure than five or ten years ago."

Friendly fraud has increased in the online channel by **41 percent** since 2011.

Friendly Fraud is a Real and Growing Problem

Friendly fraud, aka cyber shoplifting, happens when a customer makes an online purchase and then disputes the charge with the issuer. The customer may claim that the charge is fraudulent ("I didn't buy that") or that they never received the goods/services. The merchant pays dearly for friendly fraud because they must refund the disputed transaction, pay fines and fees for the chargeback and they lose out on the cost of the goods or services (and shipping).[8]

This type of cyber shoplifting is on the rise. Friendly fraud has increased in the online channel by 41 percent since 2011. On top of that, 86 percent of chargebacks are deliberate—costing merchants $11.8 billion every year.[9]

Friendly fraud is largely deliberate, and it can come in many shapes and forms:

- Cardholder claiming they did not receive merchandise
- Cardholder claiming merchandise was damaged or not as described
- Cardholder claiming they never placed the order

Some cases of friendly fraud are also unintentional, whereby a customer simply does not recognize the charge on their monthly statement and believes erroneously that fraud has occurred. This problem affects both online as well as brick-and-mortar purchases.

Why Merchants Struggle to Solve the Credit Card Fraud Problem Effectively

Friendly fraud is expected to rise as ecommerce grows and fraudsters continue to move to less secure online channels. Friendly fraud as it stands is a monumental problem for merchants. This problem is further complicated by the simple fact that the current payments ecosystem is not designed in a way that lets merchants and issuers collaborate and communicate efficiently. This lack of communication leads to information silos that cost both merchants and issuers in unnecessary operational costs and fraud losses.

This problem plays out in a number of ways.

THE PROBLEM

CARDHOLDER DOES NOT RECOGNIZE THE TRANSACTION

What do vanity license plates and credit card statement descriptors have in common? Most of the time, people have no idea what they mean. "Cardholder does not recognize transaction" represents one of the top credit card fraud reason codes, which contributes to the growing $40 billion fraud and chargeback problem. This problem is rooted in confusing billing descriptors that are almost impossible for cardholders to identify and make sense of. As a result, they file a dispute with their credit card issuer who is also in the dark about what the billing descriptor means. Confusing billing descriptors and lack of timely information being shared across the payments ecosystem lead to painful but avoidable instances of fraud, lost customers and sales for merchants.

Many merchant and issuer systems don't allow for much room to clearly define a charge on a statement. Verifi CEO Matthew Katz said that is a major factor that leads to confusing, frustration and ultimately more disputes.

"I make multiple purchase through Retailer XYZ each month. So, my credit card statement could have five, 10 or more different transactions listed for that retailer, all of which can be listed with the same description: 'Retailer XYZ.'" Katz said. "This is also true if you look at your statement online. Confusion around the charge can occur as a result because online banking and the descriptor-based system that the associations provide is very limited.

$40B

"Cardholder does not recognize transaction" represents one of the top credit card fraud reason codes, which contributes to the growing $40 billion fraud and chargeback problem.

“The association networks only allow for a 25-character descriptor to be provided by the merchant to begin with. However, each issuer may or may not even use all 25 characters, based on their policy or system-defined rules,” Katz added. “We have seen situations where certain issuers only display 23 characters and others who only use 18 characters in their online banking system. Therefore, it is incredibly challenging for merchants to convey a complete message to support the charge.”

THE PROBLEM

A TANGLED GAME OF TELEPHONE THAT COSTS EVERYONE IN LOST PROFITS

When a cardholder wants to dispute a charge, up to 86 percent of the time they contact the issuer directly, bypassing the merchant and placing the resolution emphasis on the party who largely lacks the information to adequately validate the purchase. The merchant holds all the purchase details, leaving the issuer with no recourse except to side with the customer and file a fraud claim or issue a chargeback. That’s likely after a lengthy investigation and several calls between the cardholder and issuer, not exactly the single-call resolution the cardholder was hoping for.

Since about 25 percent of e-commerce loss is related to “friendly fraud”[10] and operational costs associated with chargebacks impact merchants’ profits by up to 20 percent[11], the negative effects of not having the right information needed at the time the dispute originates adds up very quickly.

Marchand says the inhibition of natural communication between issuers and merchants is a very real problem. “Merchants and Issuers don’t typically have a natural path of communication as most payment processing activities are between the payment acquirer and the merchant. Merchants would like to better understand card issuing bank decisions when it comes to chargebacks and authorization declines, but unfortunately there is not a well defined interface to support this.”

THE PROBLEM

LAGS IN INFORMATION FLOW AGGRAVATE THE ISSUE

TC40 is raw reporting data from the issuer that contains all instances of fraud reported by issuers. TC40 includes more than just chargeback data and can help merchants evaluate their current overall fraud protection and risk management strategy as well as take steps to make it more effective. While this data has many uses, chargeback prevention is not one of them. This data comes very late in the game, and oftentimes it is misleading or not relevant to chargeback disputes. Relying on TC40s alone leads to over-refunding on transactions that don’t actually turn into chargebacks (false positives). If a merchant is using TC40 for chargeback prevention, they are likely learning about a dispute after it is too late. The result is the merchant loses the sale (which may have been legitimate), while also losing the customer and suffering losses to brand reputation and loyalty.

THE LACK-OF-INFORMATION FALLOUT:

Chargeback disputes affect the entire payments ecosystem. Issuers are under pressure from regulators aiming to protect cardholders. This has a trickle-down effect on merchants, who typically do not come out on top of disputes and end up paying fines, fees and penalties in addition to refunds and the cost of lost goods and services. They also face the loss of processing privileges if their chargeback ratio reaches 1 percent or higher for sequential months. Consumers also pay the price via the increased cost of goods and services as merchants try to recover lost profits. We've outlined the specific impacts to each party below.

ISSUERS

Issuers face increased operational costs as most disputes are processed manually and undergo an inefficient, time-consuming and error-prone process that drains resources and has a negative impact to the bottom line. This process is extremely difficult to optimize as there is no standardization within the industry; each dispute process depends on commerce channel, liability shifts, risk exposure, and operating regulations. Additionally, there are different considerations for card, ACH and alternative payment providers, increasing complexity, operational costs and fragmentation of dispute resolution outcomes leading to inconsistent customer experience. Additional negative impacts include:

WASTE OF TIME AND MONEY – Without the necessary data to quickly and accurately discuss the transaction with a cardholder, issuers find themselves in a convoluted, repetitive and expensive game of phone tag to resolve a cardholder issue. Lack of insight into transaction details limits the issuer's ability to provide clarity for the cardholder and adequately validate the legitimacy of the charge. The time and resources devoted to the investigation and eventual chargeback proceeding can be staggering, as can writing the charge off as a loss.

COMPLIANCE COSTS & INCREASED RISK – Issuers must invest in technology and staff to handle the dozens of chargeback reason codes that must be understood and managed in order to remain compliant. These reason codes are complex and changing, often requiring the implementation of new systems and processes. Additionally, issuers face elevated compliance risks, fines or legal actions, not to mention increased regulatory scrutiny and reputational damage any time there is a dispute that isn't handled quickly.

UNMANAGEABLE PEND QUEUES – The back-office handling of disputes requires a large amount of outbound documentation. As disputes increase, more experienced chargeback representatives are being called in to help with simple disputes, lowering productivity and increasing delays.

UNHAPPY CUSTOMERS – Disputes are not fun for customers, either. Cardholders dedicate time to reaching dispute resolution, often having to contact the issuer more than once to get to the bottom of the issue. Issuers overwhelmed with disputes must sometimes staff ill-prepared customer service representatives to handle disputes, even though they typically do not have any more information than the cardholder does and are not trained as chargeback representatives. This inefficiency and the lack of a speedy resolution damages the relationship between the cardholder and issuer, which hurts retention and damages the brand.

MERCHANTS

Merchants face pressure from all sides when it comes to chargeback disputes. They bear the burden of resolving disputes quickly, despite the fact that most cardholders bypass them in favor of contacting the issuer first. Sometimes a merchant doesn't even know there has been a dispute until it is far too late. Sometimes they never find out, thus limiting their ability to correct policies and procedures that would stop the same kind of disputes from emerging. Since sales volume and chargebacks are tightly coupled, it is detrimental to implement overly conservative front-end measures to stop chargebacks as it leads to lost legitimate sales and decreased profits. There are a number of ways merchants are negatively impacted by chargeback disputes:

ANTIQUATED SYSTEMS & THE OVERALL DISCONNECT – The fact that most cardholders call their issuer when they are confused by a charge on their statement is a serious problem for merchants because issuers often don't have any more information than the cardholder does and their internal systems do not communicate with those of the merchant, limiting the issuer's options to processing a chargeback.

INCREASED FRAUD – Because merchants are often in the dark when it comes to cardholder disputes, they are frequently playing an unwinnable game of catch-up, which gives individuals looking to take advantage of the lapse an avenue to acquire more money than they're entitled.

FALSE POSITIVES – Too-strict front-end fraud prevention increases false positives and manual reviews, both of which are costly and resource-draining. More importantly, this increases friction at checkout, driving away legitimate sales. It's reported that one legitimate attempt at fraud can be accompanied by up to 40 false positives.[12] In other words, up to 97 percent of transactions flagged as high-risk can be legitimate.[13]

LOST CUSTOMERS & BRAND DAMAGE – Any dispute that isn't resolved quickly is going to create a negative experience for a cardholder. A vague descriptor on a person's credit card statement might not seem like a big deal, but it can induce a painful process for the merchant, cardholder and issuer, especially if the issuer doesn't have any information beyond that confusing descriptor.

INEFFICIENCY – The financial impact of chargebacks stretches beyond the balance sheet. Chargeback disputes lead to manual processing, reconciliation and reporting and coordinating with various issuing banks. This costs merchants in time, money and additional staff.

LOST GOODS/SERVICES – Merchants typically lose out on the goods and services (as well as shipping costs) when a consumer files a chargeback. Recurring and subscription merchants feel the pain, too – intangible services rendered cannot be recovered when chargebacks occur.

PENALTIES/FINES – Merchants face fees and penalties when they exceed a chargeback rate of 1-1.5 percent for several consecutive months in order to protect consumers' best interests. In some cases, the acquirer may eliminate a merchant's payment processing privileges altogether.

How Data Sharing and Merchant and Issuers Collaboration Can Reduce the Pain

“The current chargeback process is broken,” Julie Conroy, Research Director at Aite Group said. “Issuers and merchants need an alternate set of rails that can help bridge the communication gap. If each side has more data about the transaction at their disposal, better decisions can be made and everybody wins.”

By working together, merchants and issuers can dramatically improve the quality of the customer experience and reduce the revenue loss and chargeback risks that result from gaps in the process.

Collaboration through an information-sharing platform can quickly resolve billing confusion and disputes that lead to false fraud claims, unnecessary chargebacks and lost profits in near real time.

Using a platform that facilitates order detail information sharing between merchants and issuers can help issuers validate the legitimacy of the sale with the cardholder, reconfirm the purchase or enhance identification of fraud for follow-up actions. On the merchant side, this type of platform serves as an early warning system that gives merchants real time insight into consumer dissatisfaction, enabling them to protect their brand reputation through proactive retention measures or by winning back customers and building long-term loyalty and sales.

The Issuer gains immediate insight into customer-merchant relationship (account lifespan), transaction history, dispute history and PAN/device usage history and provides the cardholder with better recognition of the charge or helps confirm a valid fraud dispute. Merchant-issuer collaboration has the following benefits:

Identify and reduce credit card fraud and friendly fraud chargebacks – With a platform to share purchase details between the cardholder, merchant and issuer, the issuer can legitimize and reconfirm the sale right away upon inquiry from the cardholder.

- This reduces instances of fraud and chargebacks due to “cardholder does not recognize transaction” or where the cardholder is seeking to fraudulently avoid paying for the item or service.
- This provides real-time insight for both merchants and issuers to identify instances of true fraud, improve fraud prevention strategies and stop pending purchases to reduce future losses.

Proactive representment – Merchant-issuer collaboration helps support the compelling evidence requirements through immediate availability of order details to prevent disputes from becoming a chargeback.

Improved operations through feedback loop – Insight obtained and passed along by the issuer handling a dispute allows the merchant to better understand which information is most impactful in solving the cardholder's problem and how to improve order processes and reduce confusion and disputes that otherwise would have escalated.

Reduce profit leakage and "double dipping" – Merchants avoid unnecessary chargeback fees, fines and operational drain processing disputes that could have been resolved directly. They also gain real-time visibility into customer outcome on disputes to prevent "double dipping" by unscrupulous customers trying to obtain more money than they are entitled. Likewise, issuers avoid resource drain from the time spent investigating disputes or writing the charge off as a loss.

Retain customers and revenue – Collaboration provides essential details to the issuer, who can immediately remove cardholder confusion by validating the purchase the cardholder made in a single call. These details reduce customer friction and allow the merchant to quickly remind customers of their purchase, increasing retention of both the customer and revenue that would otherwise be lost to chargebacks and unnecessary refunding.

Since not all disputes can be resolved on the first call to the issuer, there are some third-party systems designed to better protect merchants and issuers from the financial and reputation damage that results from lengthy dispute resolution processes and chargebacks. Verifi offers solutions that put the power to increase customer satisfaction and profits and avoid costly chargebacks with the party who can best address the dispute at the point of occurrence. These platforms provide the right information for the right parties at the right time to identify true fraud, stop chargebacks and support legitimate sales. They enable merchants and issuers to resolve disputes in a prompt and customer-friendly manner to to avoid unnecessary fees, fines or increased operational costs that happen when a dispute escalates to a chargeback. Learn more about how Verifi aligns the interests of the entire payments ecosystem – connecting top card issuers, merchants, consumers and solutions providers through unified workflow, technology and expertise at www.Verifi.com.

Conclusion

Chargebacks and credit card fraud are on the rise, especially for CNP merchants. Unfortunately, many chargebacks would be preventable with the right information-sharing between merchants and issuers. Whether they don't recognize a charge on their monthly statement or are trying to avoid paying for merchandise, cardholders tend to reach out to the issuer first to dispute a charge. Without access to detailed order information, issuers often lack the necessary information to either validate a legitimate sale or confirm that fraud has occurred, leading to lengthy dispute processes and unhappy customers for both merchants and issuers.

When merchants and issuers share order details in near real time, issuers can lower operational costs by quickly resolving disputes and thereby retaining loyal customers while validating the nature of the transaction. Merchants can also reduce internal costs associated with chargebacks, eliminate chargeback fines, fees and penalties and cut down on over-refunding. The end result is significantly lower costs associated with fraud and chargebacks as well as strengthened brand reputation and increased customer retention.

The CNP landscape continues to become more complex with emerging payments technology and regulatory requirements. The CNP channel faces increased risk that will require merchants to reconsider how they combat fraud and chargebacks in order to protect the bottom line without inhibiting legitimate sales. Merchant/issuer collaboration is the cost-effective and efficient choice to prevent avoidable disputes and proactively retain loyal customers. This type of teamwork can give all parties in the ecosystem the upper hand against increasingly shrewd fraudsters.

Visit our resource section to learn more about how you can reduce or eliminate costly chargebacks.

About Verifi

From startups to Fortune 500 companies, Verifi is equipped with the versatility to work with a wide range of industries to maximize revenues and reduce all aspects of chargeback losses. Headquartered in Los Angeles, California, Verifi processes more than $20 billion transactions each year and manages more than 12,000 accounts worldwide. With its proven team of experts and award-winning custom solutions, the Verifi Difference consistently protects merchants' payments and significantly boosts profits for the entire transaction ecosystem.

VERIFI™

Why Choose Verifi?

Partner with Verifi to reduce your payments risks, streamline business processes and lower operational costs. Whether it's stopping fraud, maximizing your billings on our flexible and robust global gateway or our award-winning chargeback prevention and dispute management services, our team of experts and custom solutions will protect your payments and boost your profits across the entire transaction lifecycle.

Contact Verifi

323.655.5789
info@Verifi.com
www.Verifi.com

Citations

1. http://pointofsale.com/2016031510048/Payment-Processing/EMV-and-Beyond-Technology-Rises-to-the-Consumer-Fraud-Challenge.html

2 http://wwd.com/retail-news/people/think-tank-bill-zielke-emv-chip-10399325/

3 http://wwd.com/retail-news/people/think-tank-bill-zielke-emv-chip-10399325/

4 http://wwd.com/retail-news/people/think-tank-bill-zielke-emv-chip-10399325/

5 http://wwd.com/retail-news/people/think-tank-bill-zielke-emv-chip-10399325/

6 http://wwd.com/retail-news/people/think-tank-bill-zielke-emv-chip-10399325/

7 http://wwd.com/retail-news/people/think-tank-bill-zielke-emv-chip-10399325/

8 http://www.digitaltransactions.net/news/story/COMMENTARY_-Don_t-Let-the-Scourge-of-_Friendly-Fraud_-Hurt-Your-Bottom-Line

9 http://www.digitaltransactions.net/news/story/COMMENTARY_-Don_t-Let-the-Scourge-of-_Friendly-Fraud_-Hurt-Your-Bottom-Line

10 https://www.merchantriskcouncil.org/resource-center/surveys/2014/2014-mrc-global-fraud-survey

11 https://www.javelinstrategy.com/coverage-area/impact-fraud-and-chargeback-management-operations

12 http://blog.finsphere.com/2013/04/19/five-words-nobody-likes-to-hear-your-credit-card-was-declined/

13 http://blog.finsphere.com/2013/04/19/five-words-nobody-likes-to-hear-your-credit-card-was-declined/