"CHIPPING" IN FOR CONSUMER PROTECTION OR CHIPPING AWAY AT SMALL BUSINESS?

DAN DAVIDSON*
STACEY TURMEL**

Credit card fraud is, and has been, a major concern for quite some time. Nowhere is this truer than in the United States. Roughly half of all credit card fraud across the globe occurs in the U.S., where only about one fourth of the world's credit card transactions occur.[1] While credit cards have been around since the early 1900s, it was not until 1966 that these cards could be used in a wide variety of locations and for multiple purposes.[2] In fact, the first credit cards were issued by oil companies and department stores for site-specific use in order to develop customer loyalty.[3]

I. THE BIRTH OF CHARGE AND CREDIT CARDS

The first bank card, Charg-It, was introduced in 1946 by a bank in Brooklyn.[4] However, it could only be used by bank account holders and was accepted by only a few local merchants. In 1950, the Diners Club card was introduced. This card also had limited usage, primarily at restaurants and hotels. It was a charge card rather than a credit card, in that cardholders were required to make payment in full every month.[5] The original Diners Club card was made of cardboard and the merchant had to write down the information on the card upon accepting it. In 1958, American Express began issuing its own "travel and entertainment" card, in order to compete with Diners Club, expanding the charge card landscape. These cards were also

* J.D. Professor of Business Law, Radford University.
** J.D., Director of the MBA Program, Radford University.
[1] Ken Sweet, *Here's why Americans are getting new credit and debit cards*, THE BIG STORY, ASSOCIATED PRESS (Oct. 1, 2015, 10:16 PM), http://bigstory.ap.org/article/eef177076bf947df9bdd2282d10a7668/heres-why-americans-are-getting-new-credit-and-debit-cards.
[2] Ben Woolsey and Emily Starbuck Gerson, *The History of Credit Cards*, CREDITCARDS.COM (last updated June 15, 2016), http://www.creditcards.com/credit-card-news/credit-cards-history-1264.php.
[3] *Id.*
[4] *Id.*
[5] *Id.*

made of cardboard, but in 1959 American Express became the first company to issue a plastic charge card.[6]

The first general purpose credit card was issued in 1966 when Bank of America launched what eventually became the "Visa" card. That same year "a national credit card system was formed when a group of credit-issuing banks joined together and created the InterBank Card Association… The ICA is now known as MasterCard Worldwide…"[7]

Both Visa and MasterCard introduced the "open-loop" credit card. These cards were intended for wide-spread use with a variety of merchants and businesses. This was a sharp contrast from the "closed loop" usage of Diners Club and American Express, and it led to a substantial increase in the use of and demand for credit cards by consumers. Where previously most consumers operated on a cash basis by paying for purchases with cash or check, now consumers could just use the card and worry about making the payment when the statement arrived at the end of the billing cycle.

II. DIVING INTO FRAUD: JUST THE FACTA MA'AM

These early cards were used with "zip-zap machines," the old-fashioned imprinter. The card was placed on a base in brackets, a form was laid over the card, and a roller was then run over the form-covered card, imprinting the raised numbers on the card on the overlain paper. The customer then signed the imprinted paper, after which the merchant gave a copy to the card-holder and routed the "original," the top sheet, to the bank. The bank would then "read it optically and manually check the number against known fraudulent accounts."[8] The bank's process could take several days to complete before the merchant would be paid.

Use of the zip-zap machine allowed wide-spread use of credit cards, but it also presented two problems. It not only delayed the payment received by the merchant that had accepted the credit card for payment, it also allowed for relatively easy credit card fraud. A customer's card could be imprinted twice (or more), once for the customer's signature to show payment, and again to gain access to the card number and expiration date. Such information could then be used by the employee of the merchant who made the second impression of the card, or sold to some willing, albeit criminal, purchaser for his or her illegal usage.

---

[6] *Id.*
[7] *Id.*
[8] Marcia Frellick, *The rise and fall of the credit card magnetic stripe*, CREDITCARDS.COM, (June 14, 2011), http://www.creditcards.com/credit-card-news/history-credit-card-magnetic-stripe-1273.php.

The receipt provided for the customer was frequently just thrown away by that customer at a later time, where a "dumpster diver" might find it in the trash. The discarded receipt also had the card number and expiration date, vital information for anyone intent on committing credit card fraud. In addition, early paper overlays had carbon paper between the original and the receipt. This carbon paper was often just discarded by the merchant, only to be available for recovery by a "dumpster diver" at a later time.

The first problem, the delay in payment to the merchant, was addressed in the 1970s with the introduction of the magnetic stripe on credit cards. The magnetic stripe on the card carried personal and financial information, it could communicate that information to the bank electronically, the bank could immediately verify whether the charge would be accepted, and the merchant was able to receive payment virtually immediately. This system, developed by IBM in the 1960s, allowed a customer to swipe his or her card through a reader. This new technology was first introduced in 1970 when it was rolled out at O'Hare Airport in Chicago by American Express, American Airlines, and IBM.[9] The development team recommended that IBM adopt the technology, and in 1973 it was available for credit cards and employee IDs. However, it was relatively expensive, costing about two dollars per card to produce, so it was not widely accepted by the credit card industry.[10] By 1980 the cost had dropped to about five cents per card to produce, at which point Visa and MasterCard began to issue the magnetic stripe cards.

Use of the magnetic stripe not only sped up the process, it also eliminated the need for a duplicate copy of the imprinted card information. Instead, the customer simply signed a form printed by the store's register, received his or her receipt – the tape with the information about the transaction – and the transaction was completed. However, there was a still a problem. The receipt provided to the customer still included the card information, the account number and the expiration date. Dumpster divers now had a new type of trash to seek in their "dives." The credit card fraud problem still existed since the card number and expiration date were readily available on the receipt, which was frequently discarded by the card holder.

The Fair and Accurate Credit Transaction Act (FACTA) of 2003[11] was an attempt to address this problem. FACTA mandates the truncation of credit card and debit card numbers on receipts. Now a receipt can only show the last five digits of the card, and it cannot show the expiration date. Of course, this requirement does not apply to transactions where the merchant uses a zip-zap machine, CNP (Card Not Presented) transactions, such as internet or telephone purchases, or those in which the card number is handwritten. It

---

[9] *Id.*
[10] *Id.*
[11] Fair and Accurate Credit Transaction Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952.

was believed that this requirement would greatly reduce the number of credit card frauds, and it has undoubtedly reduced such fraud due to dumpster diving. But that did not prevent other methods of obtaining a card-holder's personal information. Instead, it may have given many card-holders a false sense of security.

III. U.S. CREDIT CARD TECHNOLOGY: ALWAYS SKIMMING THE SURFACE

One reason that a disproportionate share of credit card fraud occurs in the U.S. is the technology used on the cards. The U.S. has continued to rely on technology that is more than fifty years old: the magnetic stripe that identified the card and its supposed user. Such cards are easily copied, allowing thieves to use the information to their benefit. Such use has been, of course, to the detriment of the card issuer. If the card owner gives proper notice of the fraud, his or her liability is limited to a maximum of $50.[12] Any amount in excess of the card holder's liability had to be covered by the merchant and the card-issuer. For frauds that occur when the user has a card the card association took the loss. The merchant was likely to have some charge-back fee from the transaction, but the liability for the fraud was on the association. When the fraud occurs in a card-not-present situation the merchant took the loss plus any other costs, including any charge-back expenses.[13]

Given the ease of copying the magnetic stripe cards, issuer decided to "up the ante." To improve the security of the magnetic stripe cards, card-issuing companies began to integrate an RFID (radio-frequency identification) chip on their credit cards. These RFID chips were thought to be much safer than the previous card. There was still a risk since these cards could also be copied. One method for copying these cards is through the use of a "skimmer," reading the information contained in the RFID chip electronically and then copying that information onto a blank RFID chip on another card. As recently as 2009, *Popular Mechanics* reported that there had been no reports of any skimming outside of a lab.[14] However, by January,

---

[12] The Fair Credit Billing Act, 15 U.S.C. § 1601 et seq. (1974) protects credit card holders, and the Electronic Fund Transfer Act, 15 U.S.C. §1693 et seq. (1978) (protects debit card holders).

[13] *Credit Card Payments: Chargebacks & Fraud Liability*, THE FRAUD PRACTICE, http://www.fraudpractice.com/fl-paychargeback.html (last visited Nov. 1, 2016).

[14] Joel Johnson, *RFID Credit Cards and Theft: Tech Clinic*, POPULAR MECHANICS (Sept. 30, 2009), http://www.popularmechanics.com/technology/security/how-to/a1142/4206464/.

2011, a mere 15 months later, CreditCards.com was warning credit customers of the dangers of skimming and how to avoid the problem.[15]

Obviously, skimmer technology has been around for a while, at least since 2011. Just two years later there was even an "app for that," a skimmer application program for smartphones that was available in 2013, and it was free! This app allowed the person using it to get the name, the account number and the expiration date on the card. It did not capture the three-digit security number on the card, but that is seldom required in face-to-face transactions.[16] Most merchant card readers are set on a very low range, allowing them to only read a card that is within a few inches of the reader. A person using a skimmer can increase the power of the unit and read another person's card from as far away as fifteen feet.[17] The information can also be read through a person's wallet, pocket, or purse. This means that a card can be read while the owner is walking down a sidewalk, standing in line at a coffee kiosk, or in any of a multitude of other places. The more disturbing fact is that he or she would not know that it had happened until strange charges started appearing on his or her monthly statement.

There are preventative steps that a card-holder can use. A person can get a wallet that is made of metal or is metal lined to prevent the effective use of a skimmer while the card is in the wallet. A person can also wrap his or her cards in aluminum foil to block a skimmer. The metal or metal-lined wallet is relatively convenient, and it will always work while the card is safely encased within the wallet. Wrapping the card in aluminum foil will also always work while the card is wrapped. And the protection provided might even make the strange looks the card-holder gets as he or she removes the card from his or her wallet, unwraps it from its aluminum cocoon, uses it, and then carefully re-wraps it before returning it to its proper place, worth the eye-rolling and head-shakes of the sales clerk.

IV. MAY THE CHIP BE WITH YOU

Now the next generation of "safe" cards is coming to America. The EMV card has been in widespread use throughout much of the world for several years, but it has been slow to enter the U.S. card market. The EMV (Eurobank, MasterCard, Visa) card has a chip embedded in it that is

---

[15] Ben Woolsey & Emily Starbuck Gerson, *Skimming 101: How to spot it, avoid it, deal with it*, CREDITCARD.COM (last updated January 6, 2011) http://www.creditcards.com/credit-card-news/credit-card-skimming-scam-1282.php.

[16] Nicole Bogart, *Smartphone app that allows credit card skimming 'real risk' to consumers: experts*, GLOBAL NEWS CANADA (April 24, 2013, 4:41 PM), http://globalnews.ca/news/508214/smartphone-app-that-allows-credit-card-skimming-real-risk-to-consumers-experts/.

[17] *Id.*

supposed to make it virtually impossible to clone and should, in theory, greatly reduce the incidents of credit card fraud in the United States. It will not eliminate such fraud, of course and said fraud still occurs in countries that already use the EMV-enabled chips. However, most other nations that use credit cards and utilize cards with EMV chips, only experience half of the credit card fraud that occurs in the US.

Card issuers are relying on two factors to reduce or eliminate their potential liability due to card fraud. The first, obviously, is the change to the card by including the EMV chip. The other factor is the shift in liability. The Payment Network's Liability Shift occurred in October, 2015. The banks and card issuers will no longer be liable for most credit card fraud as of this date. Instead, most of the liability will fall on the merchant who accepted the card as the method of payment.

Losses for card fraud in the U.S. are estimated to be $8.6 billion per year, with the losses in 2015 expected to exceed $10 billion.[18] The sheer size of these losses spurred the change to the chip card and its safer technology. The fact that there are still significant losses from card fraud is likely to have led to the Payment Network's Liability Shift. Merchants, many of whom have little choice but to accept cards as a form of payment, had virtually no leverage in this situation.

V. YOU'VE LOST THAT "COVERED" FEELING, NOW IT'S GONE, GONE, GONE

Unfortunately, while merchants have little choice but to accept the new chip cards, they may lack the funding to totally change over to its use by installing chip-compliant machines. There are an estimated fifteen million POS devices in the United States, as well as 360,000 ATMs. Each of these terminals is currently compatible with magnetic stripe / RFID technology, but few, if any, were compatible with the new chip technology as of October 1, 2015. The cost for changing the terminals over to be chip compliant is estimated to be around $7.25 billion ($6.75 billion for POS terminals and $500 million for the ATMs).[19] When these figures are added to the $1.4 billion expense to the card issuers of changing over to chip technology, the total cost is $8.65 billion![20] (CNN predicts much higher costs, estimating that it will cost the banks $8 billion to issue the new cards, and the cost to

[18] *Will Retailers be Ready for EMV by Oct 2015?*, FIS PAYMENTS LEADER (OCT. 16, 2013), http://www.paymentsleader.com/will-retailers-be-ready-for-emv-by-oct-2015/.
[19] *Id.*
[20] *Id.*

merchants to become compliant will be $25 billion.[21]). Consequently, in the United States, new credit or debit cards that are being issued with the new chip technology also continue to have the magnetic stripe. This allows those merchants who have not yet installed a new terminal to continue to accept credit and/or debit cards. However as of October 1, 2015, they will now by liable for *any* card fraud that occurs in their establishments if they are not using chip compliant terminals.

When one considers that the estimated cost for credit card fraud in 2015 will be somewhere around $10 billion, the $6.75 billion cost to merchants to replace their now out-of-date terminals with new chip compliant ones, seems less daunting. And if the new technology does significantly reduce card fraud in the future, as is predicted, the merchants should recoup the expense of upgrading to the new terminals in a relatively short time period. (The time to recoup the estimated $25 billion expenditure that CNN forecasts above would be much longer, making the investment much less attractive.)

Not surprisingly, even if every merchant in the country was to make the transition and every ATM in the country was also upgraded, the problem of credit card and debit card fraud due to skimming would not be solved. Not every card issued in this country was replaced with a new chip card by the October 1, 2015 deadline, and it is likely to be sometime in 2017 before all of the older cards have been replaced with new chip cards.[22] As long as the card issuers are still including the magnetic stripe on the new cards they issue, skimmers will still be able to illegally gain a card holder's personal information. The next round of new cards issued without a magnetic stripe will not likely be complete until year 2020 at the earliest. This means that skimmers can continue to gather information from card holders for at least another five years or longer.

Even after new cards containing a chip and lacking a magnetic stripe are in use throughout the U.S., there is still a significant concern. The U.S. is going to chip-and-signature usage. The card holder inserts his or her card into a reader, leaves it in until the transaction is complete, and then signs a receipt. This system is more secure than the swipe and sign that has been the tradition, but it is not the most secure method. Most of the rest of the world uses the chip-and-PIN method of validating a card transaction. The card holder inserts the card and enters his or her PIN (personal identification number) to validate the transaction. Without the PIN there is no validation, so a lost or stolen card cannot be used by the finder or the thief unless he or she also has access to the PIN. But a finder or a thief can attempt to use a lost

---

[21] Jose Pagliery, *You're about to get a new credit card … and it's an epic failure*, CNN MONEY (March 25, 2015, 4:25 PM), http://money.cnn.com/2015/03/25/technology/credit-card-chips-hackers/.
[22] *Id.*

or stolen card if the merchant uses the chip-and-signature verification method, trusting the fact that the sales clerk will not attempt to verify the signature of the user.

Merchants prefer the chip-and-PIN method since it provides greater security against fraud. Banks and card issuers prefer the chip-and-signature because it is easier on the consumer and less expensive. Some people also expressed concern that since Americans carry so many different cards, it would be difficult to remember the PIN for each one, potentially causing problems at check-out.

VI. THE WAVE OF THE FUTURE: CHIPS, APPLES AND ANDROIDS

The United States is the last of the G20 nations to adopt chip technology. Chip cards have been used in parts of Europe since the 1990s.[23] Today, eighty countries are either already using chip technology or are migrating to it.[24] According to EMV Connection, 99.9% of the terminals in Europe are chip-enabled; 84.7% in Canada, Latin American, and the Caribbean; 86.3% in Africa and the Middle East; and 71.7% in Asia and the Pacific.[25] Europe has been using the chip-and-PIN requirement since 2004.[26] (Many terminals in Europe no longer accept a swipe transaction.) By contrast, less than 60% of the terminals in the United States will be chip-enabled by the end of 2015.[27]

There are two main reasons for the delay in the United States in migrating to chip-enabled cards. The first is a basic difference between the U.S. market and the European market. "Bearing in mind that the U.S. is almost entirely an online authorisation (sic) ecosystem and chip and PIN was designed for a predominantly offline ecosystem, does it make sense to invest significantly to support offline PIN?"[28] The primary advantage of chip-and-PIN is preventing credit card fraud through the use of lost or stolen cards.

---

[23] Kathleen Elkins, *Why it took the US so long to adopt the credit card technology Europe has used for years*, BUSINESS INSIDER (Sept. 27, 2015, 12:30 PM), http://www.businessinsider.com/why-it-took-the-us-so-long-to-adopt-emv-2015-9.

[24] EMV FAQ, EMV CONNECTION, http://www.emv-connection.com/emv-faq/ (last visited Nov. 1, 2016).

[25] *Id.*

[26] Yasmin Ghahremani, *American travelers' 2012 guide to chip-and-PIN cards*, CREDITCARDS.COM (June 21, 2012), http://www.creditcards.com/credit-card-news/american-travelers-guide-emv-chip-cards-1271.php.

[27] *More than half of U.S. POS terminals to be EMV chip-enabled by year-end*, AITE GROUP, LLC (February 12, 2015), http://aitegroup.com/more-half-us-pos-terminals-be-emv-chip-enabled-year-end.

[28] Roger Alexander, *Chip and PIN vs. Chip and Signature: A Rivalry Nears Historic Proportions*, N>GENUITY JOURNAL (June 26, 2015), http://tsys.com/ngenuity-journal/chip-and-pin-vs-chip-and-signature-a-rivalry-nears-historic-proportions.cfm.

The use of lost or stolen cards in the U.S. is the least common type of credit card fraud, falling significantly below counterfeit cards or CNP (card not presented) transactions. (CNP transactions are primarily on-line sales.) The use of lost or stolen cards has remained relatively stable over the past three years, while fraud using counterfeit cards or fraud in a CNP transaction has increased consistently over the same time period.[29]

The second reason is less obvious, but potentially more important: The availability and growing popularity of "tap and go" payment systems using NFC (near field communication) technology. Such devices are already in use in the United States, and they are rapidly becoming a common method of payment. "Any device with an NFC smartcard chipset can very easily be configured to work as a credit or debit card."[30] For example, Apple Pay is available with an iPhone 6 or iPhone 6 Plus. Google has the Google Wallet, and Samsung products have Samsung Pay. Each has "tap and go" capability. "Virtually every mobile OS maker has their own apps that offer unique NFC functionality."[31] However, the app is only as valuable as the banks and credit cards it supports. For example, Samsung Pay supports Chase and SunTrust Banks, as well as six major credit unions, and is compatible with American Express, MasterCard and Visa.[32]

Both Apple Pay and Google Wallet provide an additional level of security to their tap and go capability; each uses a token to represent the card being used. This token does not contain the card information, instead merely identifying the customer and his or her device. The token then allows the device to communicate with the processor that processes purchases with that card. With Google Wallet, you get a "Google Wallet Virtual Card," which is a virtual card issued by Bancorp Bank. This virtual card is, in effect, a "prepaid" debit card. When the virtual card is activated, the amount of the charge is transmitted through Bancorp to the card issuer. When the charge is approved, the money is placed on the virtual card, then transferred to the merchant. The merchant gets paid, but it does not have any of the information on the customer's debit or credit card. That information is safely stored elsewhere. As a result, if the merchant should be victimized by a hacker, the customer's information will not be obtained by the hacker. He or

---

[29] *Id.*

[30] Daniel Brecht, *NFC Technology for Payments: Any Concerns?*, INFOSCE INSTITUTE (January 26, 2015), http://resources.infosecinstitute.com/nfc-technology-payments-concerns/.

[31] *Id.*

[32] Bertel King, Jr. *Samsung Pay Now Supports Chase, Suntrust, and Six Additional Credit Unions – New Users Are Eligible For A $100 Samsung.com Coupon Code*, ANDROID POLICE WEB SITE (November 23, 2015), http://www.androidpolice.com/2015/11/23/samsung-pay-now-supports-chase-suntrust-and-six-additional-credit-unions-new-users-are-eligible-for-a-100-samsung-com-coupon-code/.

she is protected from the sometimes shoddy security of the merchant. Google Wallet also required a PIN before a purchase can be authorized.

Apple Pay takes a similar approach, using a token on its device that communicates with the customer's bank, which means the customer's actual credit or debit card is used to make the payment. The Apple Pay token relies on a Device Account Number (DAN) that is unique to the customer and the device. Apple Pay also requires biometric verification before a transaction is complete. Rather than requiring the entry of a PIN, Apple Pay requires the customer to use TouchID, the customer's fingerprint, which is scanned and verifies the identification of the customer who is authorized to use that device.

Near Field Communication (NFC) seems to provide more security than credit cards, even those that have chips. The security seems to be superior to chip-and-PIN technology, and it is far superior to the magnetic stripe or the early versions of RFID cards. While there is still work to be done in improving the security features, it seems likely that in the not-too-distant future each person will be able to use tap-and-go technology to make payments with his or her smart phone or tablet. The device will replace the need to carry multiple credit cards or to worry about multiple PINs. A lost or stolen device can be remotely disabled, preventing loss beyond the value of the device itself through either of these events.

In Europe contactless payments have nearly tripled, and the number of terminals that can handle such transactions has doubled.[33] MasterCard PayPass™ and Visa payWave are now available, as well. MasterCard PayPass is available as a card, a tag, or an app for a phone.[34] Visa Europe has mandated that, effective December 31, 2015, "any terminal installation with a new Visa merchant, or any terminal infrastructure upgrade programme (sic) with an existing Visa merchant, must accept contactless payments." [35] European merchants are being warned that they must be prepared to accept contactless payments soon, even if they are unable to do so now. Those who don't will be left behind. It is likely that the United States will follow Europe quickly in moving to contactless payments, the tap-and-go method. The ease of making a purchase, the saving of so many precious seconds in the transaction, and the deepening attachment to technology almost guarantees this will occur sooner rather than later.

Will these Tap and Go payment processes using (NFC) eliminate all credit card fraud thereby obviating the need for merchant liability? Probably

---

[33] *Tap and go is the way to go*, VERIPHONE, http://lp.verifone.com/emea/tapandgo/ (last visited Nov. 1, 2016).
[34] *Your Wallet Gone Digital*, MASTERCARD, http://www.mastercard.ca/contactless.html (last visited Nov. 1, 2016).
[35] Brecht, *supra* note 30.

not. One can only speculate as to the expansion of the merchant liability framework based on Tap and Go fraud, but it is likely that the liability shift will still leave the merchant responsible for most card frauds.

VII. IN THE END: EVERYONE WINS, EXCEPT SMALL BUSINESS

Society is moving away from cash transactions. In 2011, *only* 27% of all point of sale (POS) transactions were made with cash. That percentage is declining and is expected to be down to 23% by year 2017.[36] In 2012, payments made with some version of plastic were already up to 66% sixty-six percent for POS sales, with ninety-four percent of such sales taking place in person and only six percent made on line.[37] Obviously these figures have changed considerably, with more on-line sales and fewer purchase made in person.

As recently as August, 2015, a Wells Fargo survey reported that less than half of business owners were even aware of the upcoming EMV liability shift.[38] Of those merchants accepting POS card payments, only thirty-one percent had chip-compliant terminals and only twenty-nine percent planned to install such terminals by the deadline. Meanwhile, twenty-one percent said they were never planning to upgrade.[39]

Intuit's Quickbooks website reported in April, 2015 that fifty-five percent of U.S. small businesses do not accept credit cards.[40] The cost of accepting credit cards is one of the reasons given. Included in those costs are: the cost for necessary hardware reaching as high as several thousand dollars; setting up a specific merchant-account to process the transactions; processing and transaction fees as high as four percent of each sale; chargeback fees resulting from consumer disputes; and, finally the potential liability for fraudulent use of a card.[41]

While each merchant needs to make his or her decision about accepting "plastic payments," as recently as 2013, more than two-thirds of millennials

---

[36] Catherine New, *Cash Dying As Credit Card Payments Predicted To Grow In Volume: Report*, THE HUFFINGTON POST (June 7, 2012 12:07 PM), http://www.huffingtonpost.com/2012/06/07/credit-card-payments-growth_n_1575417.html.
[37] *Id.*
[38] *Wells Fargo Survey: Many Small Businesses Not Ready for EMV Cards*, WELLS FARGO (Aug. 6, 2015), https://www.wellsfargo.com/about/press/2015/small-business-survey_0806/.
[39] *Id.*
[40] Bridgette Austin, *Cost-Benefit Analysis of Accepting Credit Cards for Your Small Business*, INTUIT QUICKBOOKS (April 13, 2015, 1:00 AM), http://quickbooks.intuit.com/r/getting-paid/cost-benefit-analysis-of-accepting-credit-cards-for-your-small-business.
[41] *Id.*

claim that they will only shop at business that accept credit cards.[42] Further, Dun and Bradstreet reported that consumers spend between twelve and eighteen percent more when paying by credit card than they do when they pay in cash.[43]

Small businesses face a dilemma: As cash purchases decline and "plastic purchases" continue to increase, they must decide whether or not to accept non-cash payments. In making this decision, each small business must do a cost-benefit analysis to determine whether it is capable of incurring the expenses for the change, and also whether it has the financial stomach to handle the potential liability from credit card fraud. In addition, each such business must recognize and plan for the inevitable movement from today's chip cards to tomorrow's tap-and-go transactions.

We are moving at Ludicrous Speed when it comes to our society's demands for instant gratification. We live in a culture that seems to "want it, buy it, have it," and give it to me *now*! There is no thought about the negative impact such a lifestyle has on ourselves, let alone anyone outside of our personal existence. No long term considerations are being given to short term buying demands and the back office fraud protection production that must be employed by the businesses that serve us. Unfortunately for small businesses, these back office software and hardware requirements can make or break their overhead, sometimes causing their businesses to fail.

So why is this important? Who cares if there is no consumer loyalty? Does it really matter if where we bought it before does not exist and we find it somewhere else? Maybe not immediately, but eventually it will. These same questions were probably asked about pollution early on in the industrial age. At the time, it may not have seemed that important to consider the impact of the pollution on our ecosystem, but eventually it hit a crisis point and everyone needed to pay attention. We are headed in the same direction regarding the imposition of credit card fraud safeguards on our small business merchants. The credit card fraud liability shifting creates a tenuous situation for small businesses and entrepreneurs trying to participate in the business marketplace. The shift of liability to the merchants basically squeezes out the little guy. Instead of only the strong will survive, it is more like only the financial mammoths will survive. It is the large companies that have the financial wherewithal to fund safeguards and absorb liability when the safeguards don't work or have been compromised.

The continuation of merchant liability in its current form could eventually leave us with fewer choices in the merchant marketplace. The

---

[42] Nathalie Pierrepont, *Survey, Small-Business Owner Still Slow to Accept Credit-Card Payments*, ENTREPRENEUR (June 20, 2013), http://www.entrepreneur.com/article/227107.
[43] Andrew Beattie, *Should You Pay In Cash*, INVESTOPEDIA, http://www.investopedia.com/articles/pf/08/pay-in-cash.asp (last visited Nov. 1, 2016).

shifting of credit card fraud liability to the merchants may, and likely will, cause some small businesses to fail. It seems that the convenience for the consumer will always prevail, but at what cost. Maybe it's time to start paying attention to the "big business" elephant in the room and its survival at the expense of our small business merchants.