Credit Cards: Risky Business or Safe Bet?

September 8, 2016 | **By Brooke Satti Charles (https://securityintelligence.com/author/brooke-satti/)**

iStock (http://www.istockphoto.com/photo/stacked-credit-cards-gm480920118-69004297?st=_p_creditcard)

Credit cards can be a fantastic way to build credit, get frequent flier miles, score points, travel internationally, receive cash back on purchases and more. As long as we use them responsibly and remain within our means, we are safe, right?

Wrong! Credit card fraud is a very real issue for financial institutions and retail companies around the world. The Nilson Report (https://www.nilsonreport.com/content_promo.php?id_promo=8) found that global fraud losses to issuers, merchants and acquirers was $16.31 billion in 2014.

It is important to note that overall card transaction volume was $28.884 trillion in 2014. This means that for every $100 in transactions, 5.65 cents was lost to fraud. The "LexisNexis Card Issuer Fraud Study (http://www.lexisnexis.com/risk/downloads/whitepaper/card-issuer-fraud-study-2016.pdf)" found that card issuers alone annually lose $10.9 billion to card fraud every year.

You are even more at risk if you live and/or conduct business in the U.S. According to a 2015 report from Barclays, 47 percent of the world's credit card fraud (http://www.securitymagazine.com/articles/86413-of-the-worlds-credit-card-fraud-happens-in-the-us) takes place in the U.S. This is interesting because only 24 percent of total credit card transactions are conducted by Americans, suggesting that a high volume of cross-border card-not-present (CNP) fraud, as well as the use of cloned foreign cards on U.S. soil.

Sluggish to Adopt Chip-and-PIN

The U.S. has begun to address this issue by adopting chip-and-PIN technology. The goal is to make it harder for fraudsters to acquire and use financial information stored on the credit card's magnetic strip. Adoption of this technology has been slow (https://securityintelligence.com/news/in-the-bag-secure-chip-and-pin-card-adoption-still-slow-in-us/), with many retailers still not accepting chip-and-PIN transactions.

A fraud liability shift went into effect in October 2015: Merchants who have not upgraded their point-of-sale (POS) machines may be liable for certain in-store counterfeit transactions. Affected merchants will no longer be able to charge back the financial institution or card issuer for lost money due to certain fraudulent purchases.

RELATED ARTICLES

Insurance, Assurance and Blockchain: Practical Steps for Market Growth (https://securityintelligence.com/macro-malware-jumping-on-the-ransomware-bandwagon/)

Read More (https://securityintelligence.com/vba-macro-malware-jumping-on-the-ransomware-bandwagon/)

Cybercrime-as-a-Service Poses a Growing Challenge (https://securityintelligence.com/as-a-service-poses-a-growing-challenge/)

Read More (https://securityintelligence.com/cybercrime-as-a-service-poses-a-growing-challenge/)

Podcast: Today's Fraud Trends, From the Dark Web to 'Pokemon Go' (https://securityintelligence.com/todays-fraud-trends-from-the-dark-web-to-pokemon-go/)

Read More (https://securityintelligence.com/podcast-todays-fraud-trends-from-the-dark-web-to-pokemon-go/)

Featured Article

Innovation Fuels IBM Q (Again) in Ga (https://securityintelligen fuels-ibm-qradar-lead gartners-2016-magic-q

By John Burnham (https://securityintellige

Upcoming Webinar

The liability shift essentially rewards the party with the most secure technology, forcing the charge back on the other party. If a counterfeit card is used in a store that has chip-enabled technology, the charge will fall on the card issuer rather than the merchant. However, if the store does not have the most secure technology, they may be liable.

Strip Versus Chip

As mentioned above, cards equipped with a chip tend to be safer than the traditional magnetic strip cards. It's easier to siphon data from magnetic strip cards via skimming devices; they are also much easier to counterfeit.

The chip is designed to be tamperproof and nearly impossible to clone, which has greatly reduced counterfeiting (https://securityintelligence.com/emv-chip-cards-a-better-way-to-pay-and-fight-fraud/) in other parts of the world where the technology has been implemented. Embedded within the magnetic strip is information such as cardholder name, account number, expiration date and CVV number.

Card-present sales, where a card is physically swiped at a merchant's POS or ATM, should become safer when retail and commercial organizations stop accepting the magnetic strip and move to chip cards.

Co-Branded Credit Cards

Co-branded credit cards are cards sponsored by two parties. Usually, one is a retail or services organization, such as an airline, hotel chain, holiday rewards organization, department store or gas chain. The other is a financial institution or credit card issuer, such as Visa, Discover, MasterCard or American Express.

In general, the bank behind the card issuer bears the true onus. It has the ultimate responsibility of deciding card approvals, determining credit limits and issuing interest rates. This means that the bank must deal with handling fraudulent charges that incur on its cards and issuing a card to a "bad debt" customer, which is a customer who becomes a liability to the issuer by not paying the balance, for example.

It is well-known in the industry that financial institutions have higher levels of security and fraud detection capabilities than most retailers. Similarly, the majority of global data breaches come from retail, internet usage, government and health care organizations.

You may be wondering why any issuer would choose to partake in co-branded credit cards. This is a legitimate question, since they bear the majority of the risk. But there are also benefits for the issuer, such as new sales channels and the potential to expand its customer base.

It is fair to say that the co-branded partner (https://thefinancebuff.com/anatomy-co-branded-credit-card.html) has the better end of the deal. It benefits from data sharing, revenue sharing, sign-up bonuses for new members, potentially higher spending and lower risks, since the issuer is assuming the majority of the financial risk. However, co-branded cards are no more or less risky than single-issuer cards.

Preventing Credit Card Fraud

Financial Institutions and card issuers take fraud very seriously. The have dedicated fraud experts and highly specialized and sophisticated security and fraud detection systems (http://www.ibm.com/software/products/en/category/advanced-fraud-protection?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US) in place that monitor unusual transaction activity.

Don't Let GDPR Blow Y
Help you S
(https://securityintelligen
let-gdpr-blow-away-5-
September 13, 2016 @ 9:30

Featured Article

Podcast: Today's Fraud
Dark Web t
(https://securityintelligen
todays-fraud-trends-fror
to-pokemon
By Security Intelligenc
(https://securityintelligence.com/author/

Featured Article

Five Critical Steps to E
Selecting an Applicatior
(https://securityintelligen
critical-steps-to-effe
selecting-an-applicatio
testing-provide
By Neil Jones (https://securityintelligence.co

Featured Article

Can Cloud Security Decr
Containment Co
(https://securityintelligen
cloud-security-decreas
containment-co
By Diana Kelley (https://securityintelligence.co

The major credit card issuers and most bank-issued credit cards have zero liability policies for unauthorized transactions on their customers' accounts, which means your bank is very likely to pay you back if it finds that your card was defrauded.

In addition, there are some practices that consumers can incorporate into their financial routine to assist in this battle:

- Keep strong financial records, and check your statements and balances often.
- Do not provide financial information to anyone unless you contacted the company directly and you are 100 percent sure it is a reputable number, contact and source.
- Do not lend out your credit cards (this includes to family, friends and children).
- Keep an eye on your cards during financial transactions.
- Immediately report suspicious activity.

For more information on keeping your credit information safe see the Federal Trade Commission's Consumer Information (https://www.consumer.ftc.gov/articles/0216-protecting-against-credit-card-fraud) page.

Tags: Credit Card Fraud (https://securityintelligence.com/tag/credit-card-fraud/) | EMV (https://securityintelligence.com/tag/emv/) | Financial Fraud (https://securityintelligence.com/tag/financial-fraud/) | Fraud (https://securityintelligence.com/tag/fraud/) | Payment Card Industry (PCI) (https://securityintelligence.com/tag/payment-card-industry-pci/) | Retail (https://securityintelligence.com/tag/retail/) | Retail Security (https://securityintelligence.com/tag/retail-security/)

Brooke Satti Charles (https://securityintelligence.com/author/brooke-satti/)

Financial Crime Prevention Strategist, IBM Security

Brooke Satti Charles is a Financial Crime Prevention Strategist within IBM Security. Her career has been focused on research and reporting of fraud, money laundering, insurance, terrorist financing, conflicts management, enterprise risk assessments, and regulatory compliance. Brooke holds a Bachelor of Science in Communication and Media Studies from Northeastern University and is currently working to achieve her Masters in Intelligence Studies.

SEE ALL POSTS →

X-FORCE RESEARCH
(HTTPS://SECURITYINTELLIGENCE.COM/CATEGORY/X-FORCE/)

MEDIA
(HTTPS://SECURITYINTELLIGENCE.COM/MEDIA/)

EVENTS & WEBINARS
(HTTPS://SECURITYINTELLIGENCE.COM/EVENTS/)

FANS
(http://facebook.com/ibmsecurity)

(http://www.linkedin.com/compa
28k
FOLLOWERS
(http://www.linkedin.com/company/ibm-security)

(http://feeds.feedburner.com/Se
1000+
SUBSCRIBERS
(http://feeds.feedburner.com/SecurityIntelligence)