Combat Rising Fraud: 5 Keys to Stemming the Tide

By John Winstel and Eric Stowell

vantiv®

smarter/faster/easier/payments™

Executive Summary

Card fraud and data breaches are a growing problem for financial institutions. The first six months of 2017 saw an increase of nearly 60% over the same period in 2016 in the sector. As fraud increases, and criminals discover new and creative ways to target financial institutions and individual cardholders alike, FIs must do more to proactively combat these attacks, and protect their cardholders.

In this white paper, we share some practical approaches to reducing fraud losses by putting your cardholders on the fraud security team.

Introduction

Imagine you get a call in the middle of the night. It's the leader of your card fraud monitoring team. A major national retailer has just announced a data breach impacting millions of consumers across the country. Your card processor has determined the breach may have impacted thousands of your cardholders.

Immediately your mind races to the steps your institution have to take now: you must notify your cardholders, decide whether to reissue thousands of cards, and analyze the potential costs of reimbursing cardholders who have suffered financial losses.

It's your worst nightmare come to life.

The growing threat of card fraud and data breaches has made this type of scenario the daily reality for card issuers. Fraud has been steadily increasing for years, with no end in sight. Financial institutions are in a constant state of anxiety, wondering when the next breach will hit.

There are proactive steps your institution can take to combat fraud and help your cardholders prepare for the worst. In this white paper, we discuss five key steps banks and credit unions can implement today to stem the tide.

Financial institutions face a growing wave of fraud

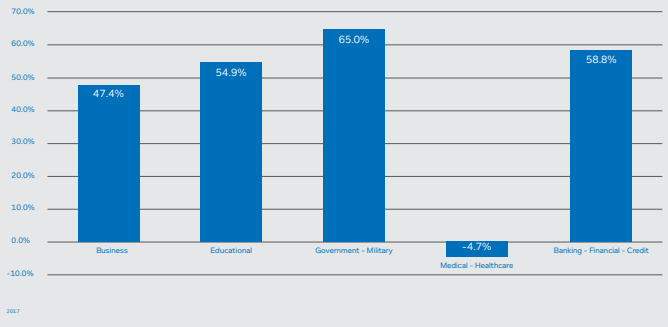
Over the past decade, international criminals have grown increasingly bold and sophisticated, targeting organizations both large and small in their quest for payoffs.

Fraud and data breaches are increasing across every industry sector. According to Aite Group, there were 2,260 data breaches worldwide in 2015. In the U.S., data breaches grew from 780 in 2015 to 1,093 in 2016, a 40% increase.

As of May 17, 2017, there have been 647 breaches YTD, a 33% increase over 2016's record 448 for the same period. [1]

Within financial services, the situation is even more concerning. Through May 2017, the sector experienced 36 breaches YTD, an increase of nearly 60% over the same period in 2016. A total of 520,000 customer records have been compromised YTD.[2] Today, card breaches are the number one source of fraud in financial services. According to an October 2016 Gallup poll, 27% of U.S. adults say they were affected by stolen credit card information over the prior twelve-month period, an increase of 22% over the same period ending in October 2015.[3]

2017 - 2016 Percent Change



Cardholders are watching the horizon

Cardholders are fully aware of the approaching tsunami, and they are concerned. According to a recent study conducted by Vantiv and Socratic Technologies, 48% of consumers have experienced card fraud at some point. In addition, an Aite Group study found that nearly half of consumers claimed an identity theft experience caused them to switch their financial institution.

Identity theft was the number one reported consumer complaint to the Federal Trade Commission for 15 consecutive years.[4] Out of 2.5 million total consumer complaints filed with or collected by the FTC, 332,646 were related to identity theft, representing 13% of all complaints in 2014.

Combine these statistics with the copious media coverage of the ongoing transition to EMV chip cards over the past few years, and it helps explain why the issues of fraud and data security are top of mind for U.S. cardholders. About half of respondents to a MasterCard survey said they have a more favorable opinion of financial institutions that offered chip cards, and one in three said they would be likely to switch card issuers if not offered a chip card by their current issuer.

Meanwhile, merchants are steadily adopting EMV technology at the point of sale. As of Oct. 2016, 2 million businesses, or 33% of all U.S. merchants have upgraded to EMV. This is a substantial increase from just 300,000 businesses in September 2015.[5]

Credit Card Theft Tops List of Crimes

Crimes more than 10% of respondents said occurred to someone in their household in last 12 months

	2014 %	2015 %	2016 %
Credit card information used at a store stolen	27	22	27
Money, property stolen	15	15	17
Identity theft	N/A	16	17
Home, car, property vandalized	14	15	14

N/A = Not asked
GALLUP CRIME SURVEY, OCT 5-9, LIST OF NINE CRIMES

1. https://www.slideshare.net/cruzcerdaphd/2017-itrc-databreach-summary-report-05172017
2. https://www.slideshare.net/cruzcerdaphd/2017-itrc-databreach-summary-report-05172017
3. http://www.gallup.com/poll/196802/americans-credit-card-information-getting-hacked.aspx
4. Federal Trade Commission, 2014 Consumer Sentinel Network Data Book.
5. http://visacorporate.tumblr.com/post/129145460088/chipcardgrowth

FIs absorb a deluge of costs

Financial institutions are absorbing the brunt of increasing costs from the rise in card fraud and data breaches. As a highly regulated industry, FIs are responsible for the reimbursement of direct cardholder losses, indirect costs related to the time and resources spent on responding to breaches, and ongoing compliance-related expenses. For these reasons, it costs financial institutions an average of $141 per record lost or stolen and an average total cost per data breach of $4 million per incident.[6]

Combating fraud presents a daunting challenge for financial institutions, one that won't recede any time soon. However, the situation is not hopeless. By taking a few practical action steps, banks and credit unions can surf the wave and develop stronger, more trusted relationships with their cardholders.

5 keys to stemming the tide

One of the most important steps your financial institution can take to minimize opportunities for card fraud and data breaches is to employ a proactive, rapid, and continuous cardholder communication strategy.

In other words, put your cardholders on your fraud security team.

Here's how:

1. Use mobile for fraud notifications

Confidence in using the mobile channel for critical and urgent communication continues to grow. In the U.S., 59% of consumers prefer to receive fraud alerts from their financial institution via a phone call, text message, and/or email to their mobile device over any other method of communication.[7]

This is great for FIs, since the mobile channel is generally the quickest way to deliver urgent and secure alerts to cardholders. Make sure you have a process in place to capture cell numbers at the time of account opening, and regular follow-up procedures to ensure you have the latest contact information for your cardholders.

2. Encourage active use of card controls

Card controls are a simple way for cardholders to monitor and set limits on specific purchase activities. Cardholders can set specific parameters customized to their individual spending habits, limiting high risk transactions based on location, merchant types, and high-dollar spending thresholds. Additionally, users can have transaction notifications sent directly to their preferred devices, allowing them to see where and how their card is being used in real time.

By encouraging your cardholders to activate card controls, you put control in their hands and instill confidence and trust in your organization. These smart precautions can also dramatically reduce fraud discovery and resolution time for your institution, reducing the probability of loss and the amount of resources spent on each incident. As your cardholders grow more confident, your card will move to the top of their wallets, and both usage and retention will increase.

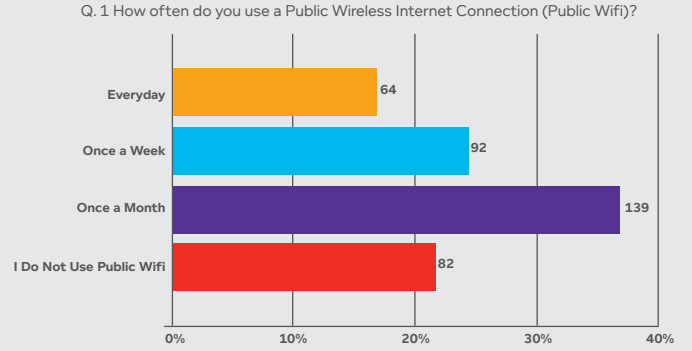
Capitalize on card controls to deputize cardholders as members of your security team.

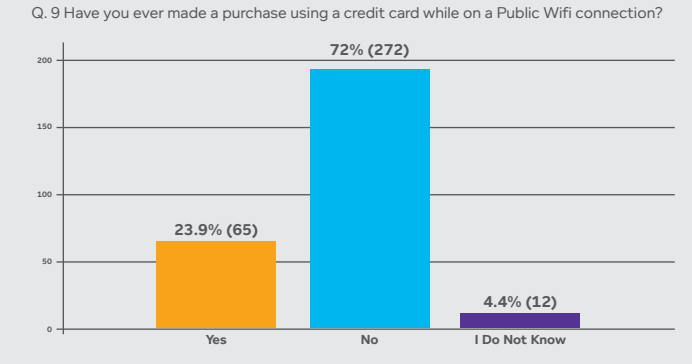
6. http://fortune.com/2016/06/15/data-breach-cost-study-ibm/
7. Global Consumer Survey: Consumer Trust and Security Perceptions, February 2017. Aite Group.

3. Educate your cardholders on how to protect themselves

One of the most effective ways to prevent fraud is through a program of regular and continuing cardholder education. Make a habit of sprinkling security tips like those listed below throughout your normal communication channels. If followed, these best practices can make a huge difference in preventing fraud:

- Review your card and bank account statements often. Don't wait until the end of the month to check your statements for signs of unauthorized activity. Log into your banking and credit card sites at least weekly to check for errors or potential fraudulent activity.
- Shred all sensitive paperwork. We all receive reams of bank account statements, credit card statements, insurance binders, and unsolicited loan offers by snail mail every month. Get in the habit of shredding these documents regularly, to discourage dumpster-divers.
- Verify HTTPS when surfing the Web. Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP, the method by which data is sent between your Internet browser and a website. The 'S' at the end of HTTPS indicates that all communications between the browser and the website are encrypted. Before entering any personal or financial information into a website, verify it has an HTTPS security designation.
- Tread carefully with public Wi-Fi. Never access financial sites or any password-protected websites using public Wi-Fi. Such networks are often open and highly unsecure. In fact, according to Kaspersky Lab, 39% of public Wi-Fi networks in the U.S. are unsecured.[8] This means that any hacker located nearby such access points can easily intercept user traffic, store sensitive data, and mine it later for purposes of identity theft or future phishing attacks. Yet, according to a 2012 survey by the Identity Theft Resource Center, nearly 24% of respondents have used a credit card to make a purchase over public Wi-Fi.[9]
- Beware of card skimming devices at ATMs. When using an ATM, be sure to inspect the machine carefully for card skimmers before inserting your card. These devices typically fit neatly over the card reader and may appear to be part of the machine. Also, always shield the keypad with your hand when entering your personal identification number. Scammers have been known to install hidden video cameras to record PINs. The safest ATMs to use are in well-lit areas adjacent to bank branches.
- Password-protect your smartphone. If your phone is lost or stolen, a complex password may be your only line of defense against someone gaining access to a treasure trove of sensitive personal and financial information. Password protection is especially important when travelling.





8. https://securelist.com/research-on-unsecured-wi-fi-networks-across-the-world/76733/
9. "Public WiFi Usage Survey," 2012, Identity Theft Resource Center, http://www.idtheftcenter.org/images/surveys_studies/PublicWiFiUsageSurvey.pdf.

4. Partner with the right processor

Above the surface, most card processing vendors seem very similar. But dive down a few feet and stark differences begin to appear. When it comes to fraud mitigation, it is critical to establish a strong and open relationship with an innovative and best-in-class card processor. Here are a few aspects to consider:

- Is your processor focused on combating fraud? The best payment processors take a multi-pronged approach to tackling fraud. Specifically, today's leading solutions employ three strategic components – People, Process, and Technology— and use advanced methods such as predictive analytics to detect fraud quickly and reliably.

  Since consumers use many different payment types, find out if your processor's fraud detection system covers multiple payment sources including credit and debit cards, wire transfers, and mobile payments. Other features to look for include transaction-based scoring and the ability to customize a fraud prevention solution to fit your individual institution's specific needs.

  Data protection requires a delicate balancing act between protecting your cardholders and conveniently serving their needs. That's where the People part of the equation comes into play. Top vendors have expert, professional fraud analysts on staff, trained to use leading-edge software to proactively manage fraud, while minimizing false positives.

- Does your processor support emerging payment types? The trend in payments is increasingly toward greater flexibility and personalization. Three popular solutions that support these preferences are mobile payments, person-to-person (P2P) payments, and EMV chip cards. Financial institutions must support these emerging payment types to attract and retain the new digital mainstream.

  According to a recent survey conducted by Vantiv and Socratic Technologies, two out of three mobile payment users believe mobile is a safer way to pay. We recommend asking your payment provider if it supports mobile proximity payments and online payments via apps and mobile websites, in addition to security features like tokenization and encryption. And don't forget to ask your vendor if it supports person-to-person payments to individuals and groups.

  The transition to EMV is an important step forward in combatting fraud. According to MasterCard fraud data, U.S. retailers who have already implemented EMV at the point of sale experienced a decrease in counterfeit fraud costs of 54 percent. Contrast this with an increase of 77% among merchants who had not yet upgraded to the technology. [10]

  Cardholders have gotten the memo. In 2016, nine out of ten Americans used chip cards regularly, a 38-percentage point increase year-over-year.[11] If your card issuer is not EMV-ready, you may not only open your institution to a higher incidence of fraud, but you may lose cardholders as well.

10. https://newsroom.mastercard.com/press-releases/mastercard-chip-momentum-reducing-fraud-one-year-in/
11. https://newsroom.mastercard.com/press-releases/mastercard-chip-momentum-reducing-fraud-one-year-in/

- Are you adding risk by using multiple vendors? If you currently use multiple payments vendors to provide credit, debit, and ATM services to your customers or members, it may make sense to consolidate your partnerships to a single provider to eliminate redundant processes and reduce fraud. By selecting a single vendor with expertise across multiple payments platforms, financial institutions have realized significant cost savings and reductions in fraud of more than 50% (see sidebar: "Empower Federal Credit Union Partners with Vantiv to Shore Up Security").

5. Promote Fraud Tools and Card Controls

Let your cardholders know you've got their back. They may not know your FI has an in-house card security team dedicated to protecting them from fraud 24/7, or that you have partnered with a vendor that provides advanced data analytics and fraud detection models to enable your institution to shut down fraudulent activity as soon as it starts.

Use a variety of communication channels, including your newsletter, website, social media, and email blasts to educate your cardholder base on all your FI does to help protect them from fraud. You may also consider offering various educational opportunities and financial advice to your cardholders, such as seminars on identity theft, fraud prevention, and protection of sensitive data. Perhaps you already offer financial planning and budgeting classes through your wealth management or investment advisory division. Don't hold back— let your cardholders know these resources are available.

Open and regular communication with cardholders offers additional benefits for your financial institution beyond helping prevent fraud and associated losses. They help enhance your brand's reputation as a consultative organization that cares about its cardholders. Continuous education will help you develop trust, uncover cross-sell opportunities, and establish deeper, more profitable cardholder relationships.

Conclusions:

Card fraud and data breaches have become a normal part of doing business in financial services. As fraud increases, and criminals discover new and creative ways to target financial institutions and individual cardholders alike, FIs must do more to proactively combat these attacks, and protect their customers and members.

Fortunately, there are some common-sense steps that can reduce the risk of fraud losses significantly. These include: incorporating mobile into your fraud notification strategy, encouraging the active use of card controls, and continuous cardholder education. In other words, by placing your cardholders on your fraud security team, you will put control in their hands, reduce fraud risk and expense, and create greater loyalty and confidence in your institution.

The key to a successful implementation of this proactive approach is partnering with a world-class card processing vendor. Look for a provider that offers innovative fraud monitoring tools and supports emerging payment types. The best solution to combating card fraud is a three-way collaboration between the cardholder, financial institution, and card processor. Through teamwork and trust, you can help stem the rising tide.

Sidebar: Empower Federal Credit Union Partners with Vantiv to Shore Up Security

Founded in 1939, Empower Federal Credit Union serves over 166,000 members across 21 locations in central New York.

Challenge: Over 78 years of operation, Empower built a reputation based on a foundation of trust and relationship-building, succeeding in part through strategic partner collaboration. However, to deliver credit, debit, and ATM services to its members, Empower found itself working with multiple payments vendors—an overly cumbersome and complicated system susceptible to fraud. Empower's executives recognized this situation needed to change.

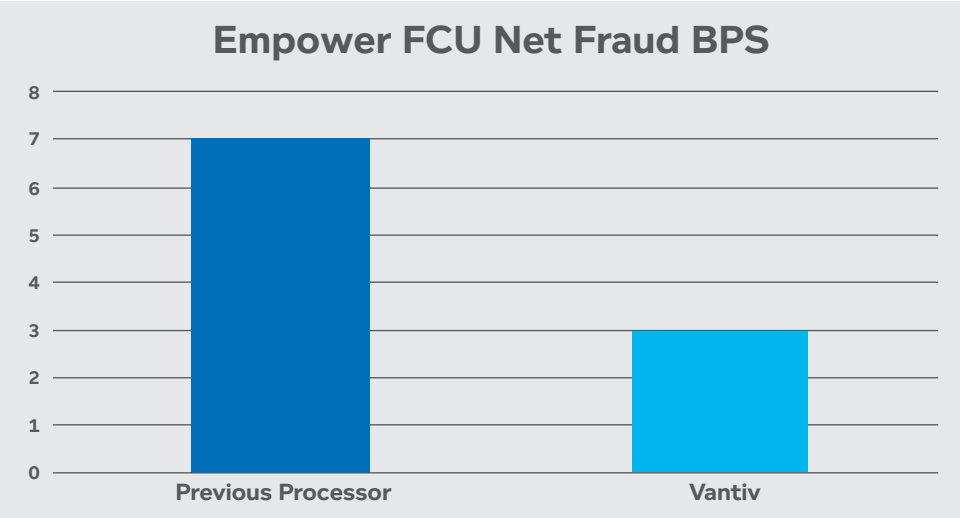
Solution: Empower collaborated with Vantiv to seamlessly integrate its loan and deposit offerings with merchant services. Through this partnership, Empower consolidated three vendor relationships into one, successfully completed a card reissue, and developed a better understanding of its cardholder base.

"The solution that Vantiv provides was more technically advanced than what we had seen from other card processors," said John Wakefield, CEO of Empower. "Vantiv takes security and fraud very seriously and brings a wealth of knowledge toward serving merchants."

Results: Through its new partnership with Vantiv, Empower has improved its efficiency and stability in several key business areas.

"Running everything under one processor for all of our card transactions probably cut our fraud losses in half with Vantiv, which is incredibly significant," explained Wakefield.

With a centralized approach to their payments offering, Empower has been able to drastically reduce their fraud risk while creating an opportunity to engage with their customers on a more personal level. "One of the reasons we picked Vantiv is because we wanted to move out into the business community," Wakefield said. "If we can be a voice and help them with their problems and help them become a better merchant, we want to be a part of that process."



"Prior to Vantiv, we were experiencing 0.07% of sales in fraud losses where now after 1 full year we are trending at 0.03% of sales" – Christine Ravas, VP of Operations for Empower Federal Credit Union

About the Authors:

John Winstel

John Winstel is a Senior Product Manager for Vantiv focusing on enterprise fraud solutions for financial institutions. John works closely with clients to understand their business needs in an effort to deliver industry leading products and services. John received his MBA from Thomas More College.

Eric Stowell

Eric Stowell is responsible for the Fraud Strategy and Analytics team for financial institutions. Eric and his team partner with Vantiv's clients and the Fraud Product division, to deliver results and minimize fraud losses. Eric has 19 years of experience in the financial services industry, with 15 of that being in credit/debit card fraud. Eric received his Bachelor's in Psychology from The University of North Texas.

About Vantiv:

Vantiv, Inc. (NYSE: VNTV) is a leading payment processor differentiated by an integrated technology platform. Winner of the 2017 NAFCU Innovation Award for its Omni Shield™ fraud protection solution, Vantiv offers a comprehensive suite of traditional and innovative payment processing and technology solutions to financial institutions and merchants of all sizes, enabling them to address their payment processing needs through a single provider. We build strong relationships with our customers, helping them become more efficient, more secure and more successful. Vantiv is the largest merchant acquirer and the largest PIN debit acquirer based on number of transactions in the U.S. The company's growth strategy includes expanding further into high-growth channels and verticals, including integrated payments, eCommerce, and merchant bank. Visit us at www.vantiv.com, or follow us on Twitter, Facebook, LinkedIn, Google+ and YouTube.

vantiv

smarter/faster/easier/payments™

VFI055 08.17