THE FUTURE OF FRAUD

Financial Institutions – Merchants – Consumers

It's Everybody's Challenge

Fraud Is on the Rise

Cyber attacks and breaches on financial institutions are becoming more prevalent

169 M

In 2015, the number of personal and financial records exposed through breaches climbed to 169 million[1]

53%

Percentage of total data breaches in 2015 related to identity theft[2]

10%

Percentage of Americans who have been victims of credit card fraud[3]

$35.54 B

In 2020, global card fraud losses will exceed $35.54 billion[4]

The Fraud Landscape

As a financial institution, your customers are your most important asset. They count on you to protect both their money and their personal information. It's a huge responsibility, especially in today's environment with identity theft rates increasing and fraudsters continually finding new ways to steal.

Defined as "deceptive practices that result in financial or other losses in the course of seemingly legitimate business transactions," many people think that fraud only affects unwitting people who are all too willing to be duped. In reality, even the savviest financial institutions fall victim to fraud.

Cyber attacks and breaches on financial institutions are becoming more prevalent, because it's so much more profitable for fraudsters than stealing directly from individual consumers. For 2015 through 2020, card fraud worldwide is expected to total $183.29 billion.[4] The effects of fraud hurt everyone – consumers, merchants and financial institutions.

Fraud Hurts Financial Institutions

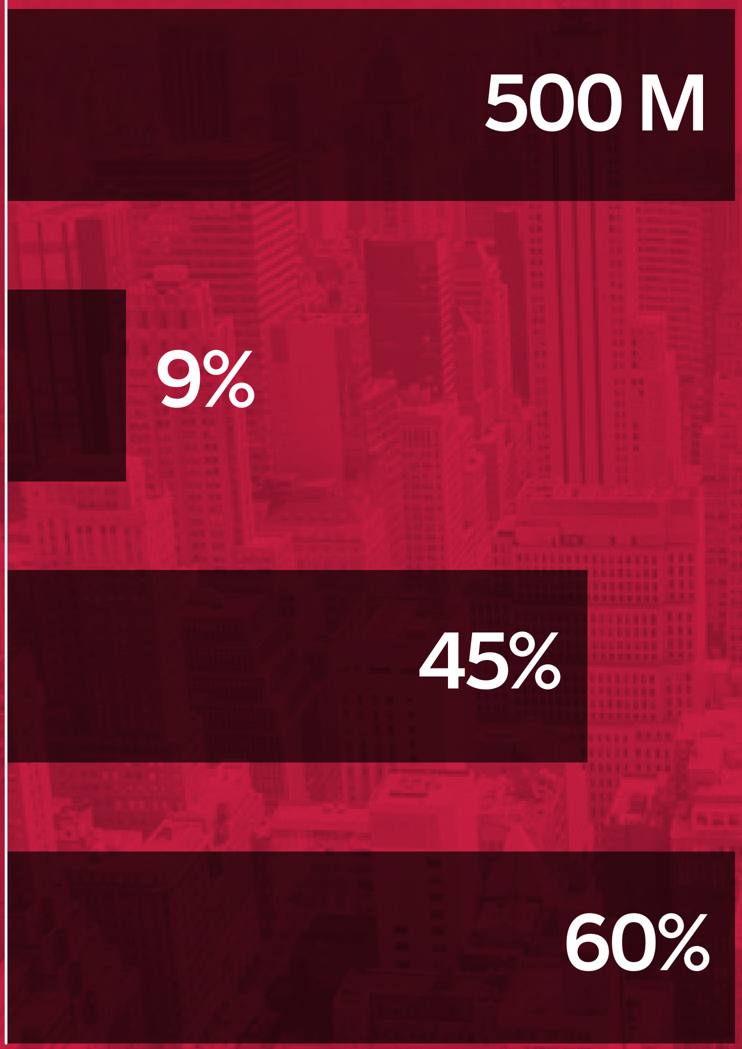
- 〉Damages brand image
- 〉Impacts reputation
- 〉Decreases customer trust and confidence
- 〉Causes loss of revenue and lowers profits

Reputational Damage
The number of records stolen from financial institutions in the past year[5]

Consumer Confidence
Percentage of American consumers who say they are "very confident" credit card issuers can keep their data secure[6]

Economic Crime
In a survey, percentage of financial institutions who reported they suffered from an economic crime[7]

Financial Responsibility
Percentage of the cost issuers are historically responsible for when a debit card is compromised[8]



Impact on Financial Institutions

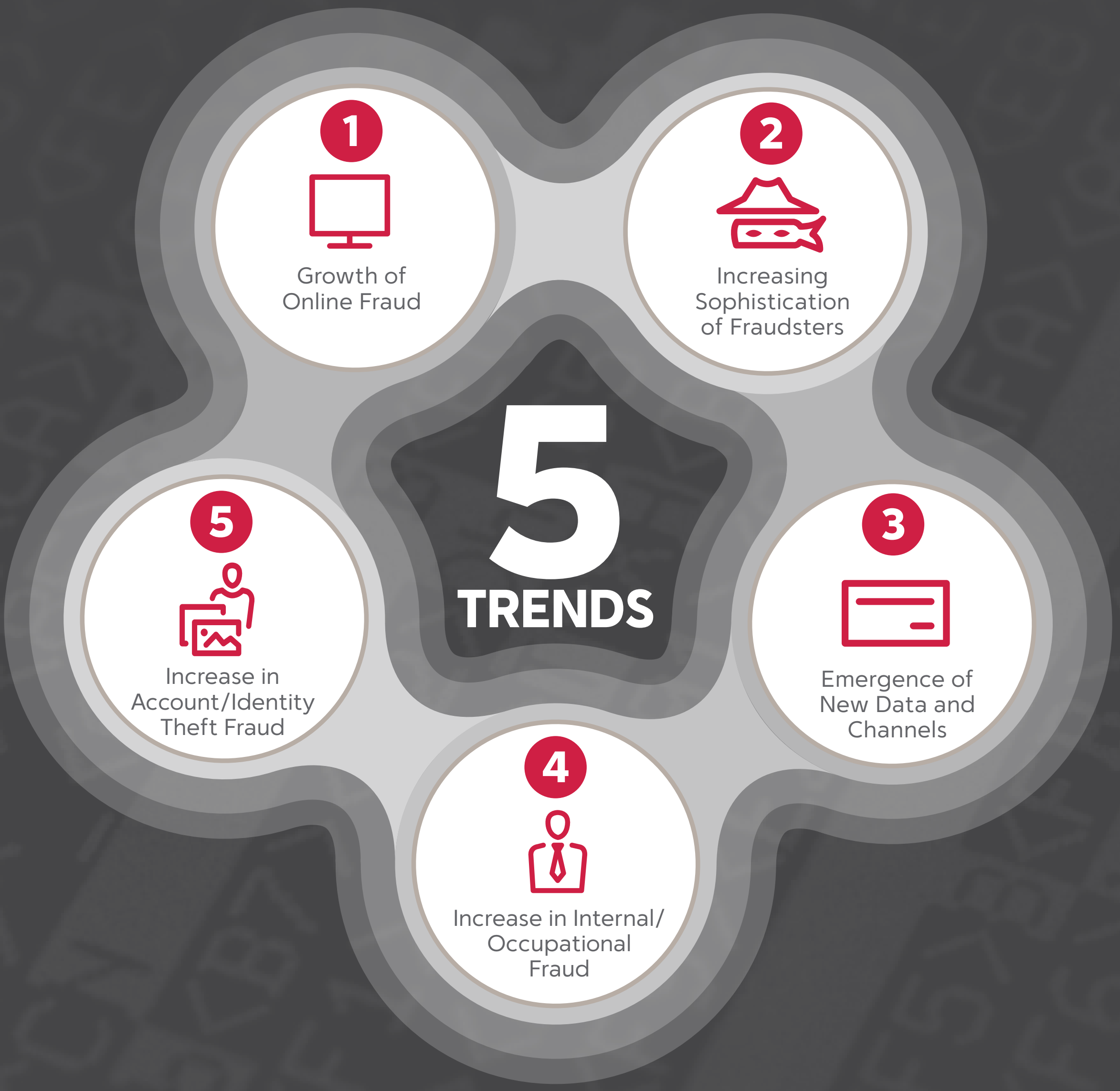
With fraud and data security threats coming in so many different forms and from so many different channels, it's crucial for your financial institution to have a strong understanding of how criminals operate and how risk management is changing. With this knowledge, along with a strategic plan, there is a better chance of mitigating risk and recognizing attacks before they do serious damage to your institution. In some cases, this may mean investing in new technologies; in others, bridging organizational silos and training staff. In all cases, it requires taking steps that help improve your institution's ability to detect threats before they reach your customer.

Build customer confidence and trust.

- ✓ Inform customers of your fraud prevention strategies
- ✓ Encourage customers to take responsibility by promoting ways they can help prevent fraud
- ✓ Educate customers on emerging fraud threats
- ✓ Provide the ability for customers to report fraud quickly and easily

5 Trends in Fraud

Threats that require more advanced strategies


5
TRENDS
1
Growth of Online Fraud
2
Increasing Sophistication of Fraudsters
3
Emergence of New Data and Channels
4
Increase in Internal/ Occupational Fraud
5
Increase in Account/Identity Theft Fraud

Trends in Fraud

Of course, traditional fraud still exists. Criminals continue to steal credit, debit and gift cards both physically and electronically and use them to pay for unauthorized goods and services; they still snatch checks and bills out of mailboxes in order to steal identities of both consumers and merchants. In today's world though, there are fraud threats that require more advanced strategies and tactics to address. Hackers, identity thieves and money launderers are focusing on different channels and spawning attacks that traditional fraud management strategies are not designed to address.

Five trends in fraud.

1 Growth of Online Fraud
2 Increasing Sophistication of Fraudsters
3 Emergence of New Data and Channels
4 Increase in Internal/Occupational Fraud
5 Increase in Account/Identity Theft Fraud

Trend #1 Growth of Online Fraud

Consumers gravitate more and more towards the internet to purchase goods and services, growing the spend volume for card-not-present activity, and so do the criminals using stolen information to rack up billions in unauthorized sales.[13]

Implement an enterprise-wide fraud management strategy.

Fraud detection, alert and case management should be managed as a whole. Centralizing your fraud management functions and ensuring all stakeholders participate, communicate and collaborate enables resources and data to be shared; capitalizes on economies of scale; and allows your institution to better coordinate tactical approaches – together this can result in reduced fraud losses and a more consistent customer experience.

Invest in the latest fraud technology and services.

STAR® Network and First Data solutions address risk and fraud across the entire customer lifecycle. **STAR Predictive Fraud Score, First Data Fraud Risk Identification Service (FRIS)** and **First Data PremierDefense**℠ can help your institution both prevent and detect transaction fraud, increasing the safety and security of every cardholder transaction.

1

Why Is Online Fraud Growing?

- Obscurity is easy with online purchases; purchasers use anonymous proxy servers and email addresses
- Fraudsters elude authorities by having items reshipped to a drop location or purchasing items online for in-store pickup
- Many eCommerce merchants do not have stringent authorization processes in place
- EMV brings greater security to brick-and-mortar POS, so, fraudsters are turning to the"card-not-present" channel[9]

7X

It's 7X more difficult to prevent fraud in remote channels than in person[10]

4X

Card-not-present fraud is expected to be nearly 4X greater than POS fraud by 2018[11]

$18.6B

Projected amount of CNP fraud in 2018 as point-of-sale fraud shrinks[12]

2

Why Is There Increasing Fraud Sophistication?

- More channels are available for fraud to occur and fraudsters to profit, so crime organizations are collaborating to capitalize on opportunities
- Technology is available that infiltrates computer networks, watching for weaknesses in security, waiting for opportunities to steal information
- Counterfeit cards are easy to create with the right tools
- Organized crime is experienced in laundering money through fake accounts

$30B

Amount of money organized crime brings in annually from "retail crime" according to the FBI[14]

$200M

Amount an "18-person crime ring" stole in one of the largest credit card schemes ever to be charged by the U.S. Department of Justice[15]

5X

Money laundering is almost 5X more likely to occur in financial institutions, and 29% of institutions believe it severely impacts their reputation[16]

13.1M

The total number of U.S. fraud victims in 2015[17]

Trend #2 Increasing Sophistication of Fraudsters

As identity theft and card fraud continue to be more profitable for thieves, there has been an evolution from casual fraudsters operating in small groups to major organized crime and international fraud rings.

Closely monitor suspicious activity.

Adjust your fraud detection engines to look for any sort of payment activity that might correspond to activity of suspected organized crime rings. It is crucial to take a proactive approach. Make sure key staff communicates about suspicious accounts and consistently monitors activity in those accounts.

Perform proactive prevention.

STAR® Predictive Fraud Score (SPFS) provides real-time, predictive fraud risk scoring powered by artificial intelligence and machine learning technology. SPFS calculates "segments of one" profiles using in-memory analytics that retain and process hundreds of millions of card profiles with transactions spanning multiple years. SPFS can help your institution prevent fraud before it happens by combining detection and prediction capabilities.

3

How Does Evolution of the Payment Channel Impact Your Fraud Mitigation?

- As the U.S. has slowly migrated to EMV, criminals have taken advantage of the learning curve
- Emerging mobile wallets utilize altering methods for the provisioning and security process
- Increased opportunities for criminals

11%

Percentage increase in fraud attacks on U.S. online merchants after the Oct. 1, 2015 EMV liability shift[18]

9 months

The time it took to discover that hundreds of EMV readers had been tampered with before being shipped to stores and supermarkets in several countries, resulting in losses in the millions[19]

215%

Amount online fraud attacks spiked for all of 2015, from 9 attacks to 27 attacks for every 1,000 online transactions[18]

Trend #3 Emergence of New Data and Channels

The ecosystem is more complicated with the new EMV card type and mobile wallets, and criminals exploit complication. When global networks mandated that merchants and financial institutions in the United States adopt EMV technology, there were varied requirements for signature and PIN use rather than the more secure PIN and chip approach used elsewhere. Mobile wallets have utilized varying methods for provisioning and security.

Take a proactive approach.

Utilize next-generation tools such as First Data's **Risk Analytics** solution, to evaluate the level of risk during the card-not-present transaction and only engage the consumer in step-up authentication, if needed, to secure the channel.

Use data analytics for fraud detection.

The **First Data Fraud Risk Identification Service (FRIS),** and **PremierDefense℠** service work to augment your expertise with subject matter experts who monitor emerging trends and analyze fraud that impacts your portfolio as well as the consortium of users, working to mitigate your losses with proactive, customized updates to rules for real-time authorization decisioning and scoring.

4

Why Internal Fraud?

According to the Association of Certified Fraud Examiners, even though the financial industry is one of the most regulated and has many controls in place, financial institutions are still getting hit with the highest rates of internal fraud[20]

40%

Percentage of internal banking fraud cases detected by a tip – twice the rate of any other detection method[21]

18 months

Average amount of time it takes to detect internal fraud[21]

75%

Percentage of insider fraud from individuals working in accounting, operations, sales, upper management, customer service, purchasing and finance[20]

Trend #4 Increase in Internal/ Occupational Fraud

Establish ethics and codes of conduct.

Requiring fraud and ethics training at least once a year sends a strong message to employees about your institution's commitment to reducing fraud. It also helps ensure your employees are up-to-date on the latest trends in fraud so that they are better able to identify potential risks.

Conduct surprise internal audits.

Most employees who commit fraud are first-time offenders with clean employment histories. They would likely steer clear of committing fraud if they had any fear that they might get caught. The **First Data FOOTPRINTS® Online** solution provides a systematic way to monitor internal transactions and detect potentially fraudulent activity by employees on cardholder accounts.

Employee training and fraud activity hotline.

Teach employees how to spot fraudulent activity and recognize "red flags," like financial need, that indicate an employee might commit fraud. Set up a hotline as an anonymous reporting system that allows employees to give tips without fear of repercussion.

5

Why Account and Identity Fraud?

As financial institutions continue to make improvements in online security and card protection technology, more fraudsters are turning to identity theft as an alternative money-making scheme

15 YEARS

Identity theft has been the #1 consumer complaint for 15 years[1]

113%

Percentage increase in new account fraud in 2015[22]

$112 B

Amount fraudsters have stolen in the past six years, which equals $35,600 per minute[23]

Trend #5 Increase in Account/Identity Theft Fraud

Invest in and deploy identity verification technology.

First Data fraud solutions include features to help confirm the identity of account holders. Authentication tools, such as **Verified by VISA**®, **MasterCard**® **SecureCode**™ and **First Data Risk Analytics**, are designed to help your institution minimize identity theft risk. In addition, First Data's **Consumer Alerts** solution offers a means to engage consumers in the proactive monitoring of activity they define as suspicious.

Limit use and storage of sensitive cardholder data within your system.

To combat external fraud, make sure access to customers' personal cardholder data is only available within applications that directly pertain to payments (transaction authentication and daily settlements, for example). In order to deter internal fraud, set up controls that limit access to customer information to only those employees whose jobs require it, and do periodic spot checks to ensure procedures are being followed.

Want to Learn More?

Call **866-380-9867** or visit **STAR.com** to find out how STAR® and First Data can help your financial institution combat fraud.

Summary

While there is no single guaranteed solution to eradicate fraud, everyone – consumers, merchants and financial institutions – plays a role in helping to both prevent and detect it.

The role of the financial institution is the most crucial. As a result, you have a responsibility to have a solid, proactive fraud management strategy that utilizes the most current fraud detention and prevention technologies. To maintain trust and confidence, you must constantly educate employees, provide information and tools that help protect individual customers and merchants – and continually invest in the most modern, innovative technologies available to help keep funds and data secure.

It's a daunting task, and that's where we come in. We're dedicated to delivering solutions that provide the strongest defense against fraud, and partnering with financial institutions to help them build best-practice, end-to-end fraud management programs. Our solutions not only support the financial institution's fight against fraud, they also protect at the consumer and merchant level.

Want to learn more?

Call **866-380-9867** or visit **STAR.com** to find out how STAR and First Data can help your financial institution combat fraud.

Sources

1. http://www.iii.org/fact-statistic/identity-theft-and-cybercrime
2. http://www.nasdaq.com/article/infographic-data-breaches-grow-more-personal-cm587750
3. http://www.statisticbrain.com/credit-card-fraud-statistics/
4. http://www.businesswire.com/news/home/20150804007054/en/Global-Card-Fraud-Losses-Reach-16.31-Billion
5. https://securityintelligence.com/the-damage-of-a-security-breach-financial-institutions-face-monetary-reputational-losses/
6. http://www.nasdaq.com/article/credit-card-fraud-and-id-theft-statistics-cm520388
7. https://www.pwc.com/gx/en/financial-services/publications/assets/pwc-gecs-2014-threats-to-the-financial-services-sector.pdf
8. https://www.nerdwallet.com/blog/credit-cards/merchants-victims-credit-card-fraud/
9. http://paymentweek.com/2016-1-12-what-you-need-to-know-about-card-not-present-fraud-9360/
10. https://www.lexisnexis.com/risk/downloads/assets/true-cost-of-fraud-2015-study.pdf
11. http://www.mobilepaymentstoday.com/articles/whats-ahead-for-online-fraud-in-2016/
12. https://www.javelinstrategy.com/press-release/cnp-fraud-rapidly-rising-irrespective-emv-adoption
13. http://www.businessinsider.com/online-fraud-attacks-in-the-us-are-growing-at-an-alarming-rate-2016-4
14. https://fas.org/sgp/crs/misc/R41118.pdf
15. https://archives.fbi.gov/archives/newark/press-releases/2013/eighteen-people-charged-in-international-200-million-credit-card-fraud-scam
16. http://www.pwc.com/gx/en/industries/financial-services/publications/global-economic-crime-survey-2014-financial-services.html
17. https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point
18. http://www.cutimes.com/2016/04/20/card-not-present-fraud-swells-11-study
19. http://www.telegraph.co.uk/news/uknews/law-and-order/3173346/Chip-and-pin-scam-has-netted-millions-from-British-shoppers.html
20. http://www.acfe.com/rttn2016/docs/2016-report-to-the-nations.pdf
21. http://ibat.org/news/2014/09/04/bank-fraud
22. http://www.cnbc.com/2016/02/02/how-fraudsters-are-getting-around-chip-n-pin-cards.html
23. http://www.cardhub.com/edu/credit-debit-card-fraud-statistics/