First Data

A First Data White Paper

FACTA: Turning Regulatory Compliance into Business Growth

Achieving FACTA Red Flag compliance while improving efficiency and boosting customer satisfaction

By Krista Tedder
Product Owner, Fraud & Risk Management

and

Glen Wordekemper
Vice President, Product Development

Executive Summary

Customer trust. It's a valuable asset that every organization works hard to build and safeguard. However, as identity theft, phishing scams and security breaches continue to proliferate, companies—especially those in the financial services industry—run the risk of damaging hard-won customer confidence and the bottom line. According to a 2007 study by Javelin Strategy and Research, an estimated 150 million U.S. consumers won't bank online due to concerns like identity theft.

The August 2008 arrests of eleven alleged hackers accused of stealing more than 40 million credit and debit card numbers highlight what those in the intelligence community have known for years—there is a mature multi-billion dollar industry created by identity thieves. In fact, in 2008, it's estimated that more than eight million U.S. adults will be victims of identity fraud.

Here's the bottom line:

Each day that an institution doesn't have an effective identity theft prevention program in place, the odds increase that the company will be damaged by fraudulent activities and the loss of customer faith.

To help mitigate the costly effects of identity theft, the Fair and Accurate Credit Transactions Act (FACTA) was introduced in 2003. In addition to addressing consumer identity theft risks, it was created to ensure fair and accurate credit reporting by consumer reporting agencies, users of consumer reports and furnishers of information to consumer reporting agencies. To further strengthen FACTA, the Federal Trade Commission and various federal financial agencies added what are known as the "Red Flag" regulations which require certain creditors and financial institutions to implement identity theft prevention programs.

Thankfully, there's no need for panic. Today, there are automated, end-to-end fraud prevention and protection solutions available to help companies ease the transition to compliance. These range from credit and debit card fraud protection to strategic customer data management solutions that can help organizations reduce the risk of lost customer trust, stiff penalties and the potentially crippling effects of a serious security breach.

This paper explores the threats of identity theft, the facts and challenges of FACTA compliance and best practices in reducing identity fraud. It also identifies solutions that will automate compliance procedures today and better prepare organizations for tomorrow. In short, this paper will help companies gain a deeper understanding of identity theft and how they can use compliance measures to strengthen customer trust.

Introduction

On November 1st, 2008, compliance with the FACTA Red Flag rules will become mandatory. Companies without a written identity theft program in place are scrambling to meet the compliance deadline. While the Red Flag rules certainly force companies to put procedures in place to ensure compliance, they will also help businesses reduce the risk of identity fraud and improve customer relations. In this shaky economic climate—hot on the heels of a major mortgage crisis—many consumers have lost confidence in financial institutions. Consumers question the safety of their valuable personal information. Losing consumer faith in your organization on several fronts can damage your brand integrity and decrease your revenue. FACTA compliance offers a step forward in rebuilding consumer trust.

The good news is that according to Javelin's 2008 Identity Fraud Survey Report, identity fraud is dropping in the United States—down an estimated 12 percent over the previous year, which translates into a total fraud reduction of $6.4 billion. Moreover, fraudulent new account openings are also down over the previous year, with average fraud amounts also dropping significantly. To stay one step ahead of identity thieves—along with the ever-changing federal and industry regulations—financial institutions need to automate their identity theft processes to mitigate costs and provide faster, more timely procedures that increase customer satisfaction.

However, according to a 2008 Information Media Group Survey, just one-half of U.S. financial institutions report they'll be ready for the November deadline, and only 3 percent are already completely compliant. In addition, many of these institutions question the effectiveness of new identity theft prevention programs, with only 20 percent projecting that new programs will be effective. Sixty-nine percent believe they will be moderately effective.

To help companies streamline their valuable information processes, meet compliance regulations and restore customer faith, there are automated, end-to-end fraud prevention and protection solutions available to ease the transition to compliance. Financial institutions have a tremendous opportunity to build market share and reassure customers that their identities—and valuable financial information—are secure.

What is Identity Theft?

Identity theft occurs when a criminal obtains key pieces of personal information, such as Social Security numbers, addresses and driver's license numbers, in order to impersonate someone else. The information can then be used to obtain credit, merchandise and services in the name of the victim, or to provide the criminal with false credentials.

Identity theft falls into two distinct categories: true name identity theft and account takeover identity theft.

True name identity theft

True name identity theft means that the thief uses someone else's personal information to open new accounts. These could be new credit card accounts, mobile phone service or new checking accounts—complete with blank checks.

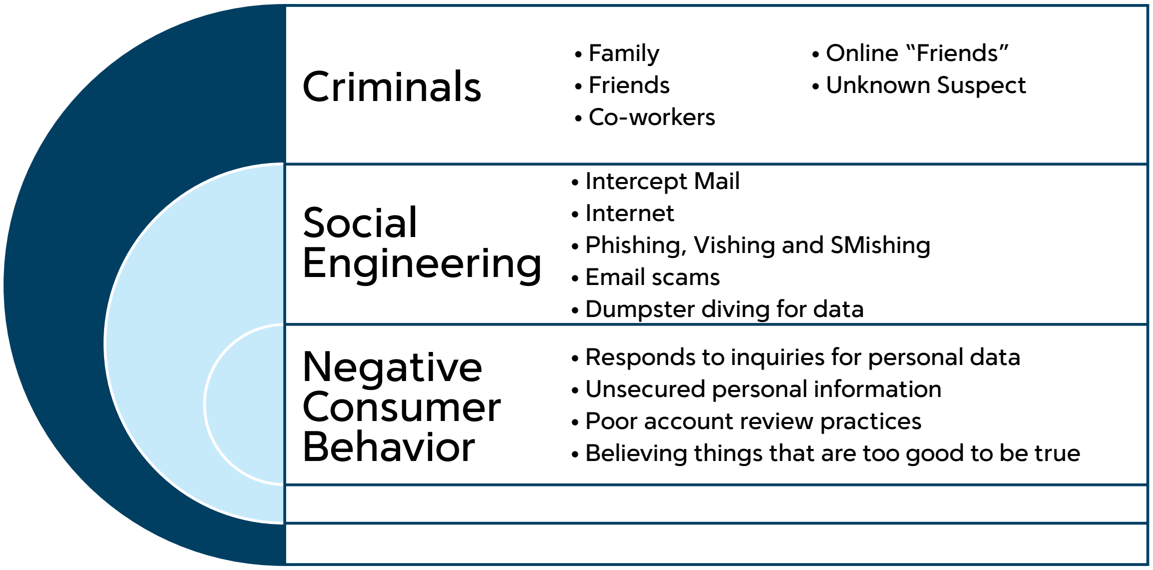
Account takeover identity theft

Account takeover identity theft means the imposter uses someone else's personal information to gain access to the person's existing accounts. A typical tactic is to change the mailing address on an account, order checks and replacement cards, and charge large sums before the person whose identity has been stolen realizes that there is a problem.

How do imposters obtain this valuable personal information in the first place? Although an identity thief might breach a database's security to obtain information, thieves have a much easier time gathering information using old-fashioned methods such as finding personal papers, discarded credit card offers, canceled checks and financial statements from a home or company's trash dumpsters. Based on the 2008 Javelin study on identity theft, approximately 30 percent of all identity theft is perpetrated by someone the victim knows. Thieves also steal bank statements, credit card solicitations and new boxes of checks directly from mailboxes. And of course, a lost or stolen wallet is a gold mine for fraud perpetrators.

Cycle of Identity Theft

Identity thieves wishing to go the high-tech route frequently use "phishing" scams wherein they send official looking e-mails to individuals requesting verification of account numbers, passwords, Social Security numbers and other key identifying information. Because consumers mistakenly believe the e-mail is from a trusted financial institution or merchant, they click on the provided link and fill in the requested information, which lands right in the hands of the identity thief. Once a consumer has unknowingly entered the fake Web site, the thief can also utilize keystroke detecting applications or other malicious software to continue to capture vital personal information.



Criminals

- Family
- Friends
- Co-workers
- Online "Friends"
- Unknown Suspect

Social Engineering

- Intercept Mail
- Internet
- Phishing, Vishing and SMishing
- Email scams
- Dumpster diving for data

Negative Consumer Behavior

- Responds to inquiries for personal data
- Unsecured personal information
- Poor account review practices
- Believing things that are too good to be true

Vishing: a new danger in identity fraud

Identity thieves are now turning to the telephone channel to steal information, increasingly using such methods as vishing. A combination of the words "voice" and "phishing," vishing uses a voice over IP (VoIP) phone to steal the victim's information. War dialers, which are modems that are able to blanket an entire region or area code with telephone calls, are often used, as well, for mass effect.

In a typical scenario, the victim receives a phone call saying that their credit card information has been compromised and they need to call a certain number. Upon connecting to the other number, the victim is asked to input their information (credit card number, PIN, expiration dates, etc.) using the telephone's keypad. The VoIP device being used is able to pick up the keystrokes made on the telephone, and thus the victim's sensitive information has been illegally acquired. The "visher" now has all he or she needs to access the victim's accounts.

In its 2007 Identity Fraud Survey Report, Javelin predicted this fraud technique as a growing threat to institutions and consumers. Yet, in 2007, only 48 percent of the top 25 financial institutions had implemented two-factor authentication for telephone banking, with many financial institutions still continuing to authenticate their customers by prompting for their full Social Security number or bank account number.

Who's targeted in identity theft?

The Identity Theft Assistance Center (ITAC) is a nonprofit organization that helps victims by streamlining the recovery process, and shares its expertise with consumers and businesses to help protect customers from identity theft. Protecting personal information is vital in maintaining trust with consumers. ITAC works with the Federal Trade Commission (FTC) and several industry organizations, such as BITS and The Financial Services Roundtable, to create and distribute reference materials to ensure that illegal acquisition of consumer data does not happen.

Findings from ITAC's Identity Theft Database reveal that two out of three identity theft victims are age 40 and older: the consumers who are more actively consuming credit and have long credit bureau histories are most targeted. This demographic typically has acquired a mortgage and is satisfactorily maintaining existing credit accounts. Their credit histories are usually good and do not often warrant extensive credit reviews. These consumers also typically are not monitoring their credit reports because they are not in the market for new loan products.

The most likely victims of identity theft are consumers who are active users of financial products and are your most valuable customers. Two-thirds of all victims are 40 years of age or older.

An analysis of 11,000 cases of identity theft showed that:

- → 12 percent of victims were ages 18 to 29
- → 19 percent of victims were ages 30 to 39
- → 24 percent of victims were ages 40 to 49
- → 23 percent of victims were ages 50 to 59
- → 22 percent of victims were ages 60 and over

Moreover, only two out of five victims know the source of the crime. Of a survey of 275 cases, 160 consumers (nearly 60 percent) did not know the source of their identity theft. In addition to helping consumers deal with identity fraud, ITAC is also a valuable ally for businesses trying to combat this serious crime. With identity theft continuing to affect so many consumers, financial institutions have more responsibility than ever to maintain and protect sensitive personal information. ITAC offers numerous resources to help businesses safeguard the foundation of trust that exists between them and their customers.

What are the costs?

While the costs of identity fraud have decreased over the years due to new regulations and security measures, they still remain high for all involved—including financial institutions, merchants and victims. In its 2008 Identity Fraud Survey Report, Javelin summarized the costs of identity fraud in new accounts, all existing accounts and existing credit and debt card accounts.

Figure 1. Incidence Rates and Average Fraud Amounts for New Accounts by Year

	New Accounts		
	2008	**2007**	**2006**
Incidence Rates Last 12 months	0.95%	1.05%	1.52%
Total Annual Cost (in billions)	$14.7	$18.5	$25.0
Mean Fraud Amount	$8,071	$7,261	$10,539
Median Fraud Amount	$3,000	$3,000	$3,000
Mean Consumer Cost	$1,066	$792	$881
Median Consumer Cost	$0	$0	$0
Mean Resolution Hours	49 hrs.	40 hrs.	77 hrs.
Median Resolutions Hours	25 hrs.	5 hrs.	25 hrs.
		© 2008 Javelin Strategy & Research	

Figure 2. Incidence Rates and Average Fraud Amounts for All Existing Accounts by Year

	All Existing Accounts (Card & Non-Card Accounts)		
	2008	**2007**	**2006**
Incidence Rates Last 12 months	2.62%	2.69%	2.48%
Total Annual Cost (in billions)	$30.6	$32.4	$33
Mean Fraud Amount	$5,229	$4,118	$7,302
Median Fraud Amount	$750	$750	$750
Mean Consumer Cost	$745	$608	$520
Median Consumer Cost	$0	$0	$0
Mean Resolution Hours	26 hrs.	24 hrs.	43 hrs.
Median Resolutions Hours	5 hrs.	5 hrs.	25 hrs.
		© 2008 Javelin Strategy & Research	

Figure 3. Incidence Rates and Average Fraud Amounts for Existing Card Accounts vs. Existing Non-Card Accounts by Year

	Existing Card Accounts			Existing Non-Card Accounts		
	2008	2007	2006	2008	2007	2006
Incidence Rates Last 12 months	1.97%	2.05%	1.82%	0.65%	0.64%	0.66%
Total Annual Cost	$18.3	$20.7	$20	$12.3	$11.8	$12
Mean Fraud Amount	$4,885	$4,279	$7,155	$9,848	$7,825	$11,935
Median Fraud Amount	$750	$750	$750	$3,000	$3,000	$3,000
Mean Consumer Cost	$632	$631	$534	$1,646	$679	$936
Median Consumer Cost	$0	$0	$0	$0	$0	$0
Mean Resolution Hours	23 hrs.	22 hrs.	40 hrs.	46 hrs.	48 hrs.	66 hrs.
Median Resolutions Hours	5 hrs.	5 hrs.	5 hrs.	25 hrs.	25 hrs.	25 hrs.

© 2008 Javelin Strategy & Research

Identity thieves are continuing to use fraudulent address changes as the preferred method for taking control of existing accounts. Javelin notes that address changes are used more than three times as often as changing a phone number or obtaining a counterfeit card. The financial losses experienced by fraudulent address changes are significant, with an average fraud amount of $13,872 for businesses—double that of 2007—and consumer costs of $2,025 per incident. The fraudulent change of e-mail address has the lowest incidence, accounting for only nine percent of account takeover cases. As a result, the FACTA Red Flag regulations focus on changing the way financial institutions handle address changes among other items.

New accounts fraud is the most difficult type of fraud to detect and can have the greatest impact on the victim, in both time and money. The Javelin survey found that it typically takes 217 days to detect new accounts fraud, and that such fraud costs the consumer an average of $1,066 per incident in 2008—a 30 percent increase over 2007. What has also increased is resolution time, growing 23 percent in 2008 to 49 hours per incident.

For those financial institutions that fail to properly secure their vital customer information or validate consumer account changes and activity, the consequences can be severe. The risks from poor security include theft, interruptions of service, physical damage, compromised system integrity, unauthorized disclosure of proprietary corporate information, penalties from regulators, civil lawsuits and loss of customers' trust.

However, the cost of identity theft is not just what it takes to implement an identity theft prevention program, pay fines and penalties for non-compliance, or replace stolen funds. Understanding the true costs means assessing compliance practices in light of the total cost of compliance (including the company's risk exposure), coming up with efficient ways of measuring the effectiveness of compliance efforts and creating a compliance governance structure that allows organizations to maximize their investments and plan for the future. This is truly an opportunity for financial institutions to turn their investments into a strategic marketing advantage by promoting these efforts to their client base.

Reducing Identity Theft Through Compliance

To address the growing consumer identity theft risks, the Fair and Accurate Credit Transactions Act of 2003 (FACTA) was enacted to amend the Fair Credit Reporting Act (FCRA). FACTA was created to ensure fair and accurate credit reporting by consumer reporting agencies, users of consumer reports and furnishers of information to consumer reporting agencies.

On November 1, 2007, the Federal Deposit Insurance Corp., Federal Trade Commission, Office of the Comptroller of the Currency, Federal Reserve and other regulatory agencies adopted the final rules for FACTA sections 114 and 315, which are also known as the Red Flag rules:

- → **Section 114** of FACTA enables the requirement that financial institutions and creditors establish a written identity theft prevention program designed to "detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account."
- → **Section 315** deals with identity theft in the new account environment, especially when there is a discrepancy between the consumer address on an application and the address held on file by the credit bureau. Because identity thieves commonly attempt to open new credit accounts at a different address than where their victim resides, Section 315 enables the requirement that a creditor first must form a reasonable belief of "true identity" when it discovers an address mismatch between the application and what is on record.

Meeting Red Flag requirements

To meet the Red Flag requirements addressed in the FACTA regulations, an institution's written identity theft prevention program must be approved and overseen by its board of directors (or an appropriate committee thereof) and include procedures that are:

- → Designed to detect, prevent and mitigate identity theft in connection with a covered account
- → Fit the size and complexity of the institution and nature and scope of its activities
- → Contain reasonable policies and procedures that cover the following four elements:
  - Identify relevant Red Flags for covered accounts and incorporate those into the program
  - Detect Red Flags that have been incorporated into the program
  - Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft
  - Ensure the program is updated periodically to address changing risks

Guidance for an identity theft prevention program

FACTA's Red Flag regulations set the groundwork for financial institutions and creditors to formally prepare and adopt an identity theft prevention program. The guidelines recommend that each institution evaluates the following factors in identifying relevant red flags for covered accounts:

- → The types of covered accounts it offers or maintains
- → The methods it provides to open these covered accounts
- → The methods it provides to access these covered accounts
- → Its previous experiences with identity theft

Based on the data collected from this evaluation, each institution will be expected to conduct a risk assessment and take appropriate action. Institutions are also expected to train relevant staff on the program and exercise appropriate and effective oversight of service provider arrangements.

Challenges of FACTA compliance

With all new regulations come challenges in how corporations meet compliance demands. Geographical location, size of organization, type of institution and a variety of other factors all play a role. In its 2008 Identity Fraud Survey Report, Javelin reported regional fraud incidence rate statistics (averaged over three years), with respondents in California, Illinois, Idaho, West Virginia and Delaware reporting the highest incidence of identity fraud. On average, New England and the Midwest reported the fewest incidents of fraud. Generally, states with dense metropolitan areas, such as California, are more likely to have higher fraud rates, due to higher income levels and commerce activity.

Complying with federal Red Flag rules requires significant policy coordination and documentation. It touches different aspects throughout an organization—from the executive offices and IT, to branch employees and call center operators. Not everyone may follow the same procedures to properly assess risk, so each department and existing policy should be evaluated during the FACTA Red Flag risk assessment.

For larger financial institutions, complying with regulations is a more significant task, but also a more familiar one. National and international organizations have the resources, technologies, policies and procedures, and support in place to facilitate regulatory compliance. However, these organizations may not have automated protection and prevention management services in place to promote automatic and consistent compliance across the enterprise.

For smaller banks and credit unions, complying presents different challenges. Given their size, these organizations must do more with fewer resources available to them, so any new regulation can be burdensome. Small institutions may not know how to develop an identity theft prevention program to comply with FACTA Red Flag rules. For these organizations, finding a risk and fraud solution that meets both their compliance and budgetary needs is paramount.

Whether financial institutions are large or small, compliance will be mandatory and challenging even for the most prepared. For example, many companies with compliance policies in place may only have to document existing procedures rather than implement a new program from scratch. However, Red Flag rules now require even these companies to combine all compliance procedures under one policy and cross reference all policies and procedures so that anyone—from corporate officers, regulatory officials, shareholders or even customers—can see what the institution is doing to mitigate the risk of identity theft.

Implementing an Identity Theft Prevention Program

Recommendations for successful compliance

According to research organization Gartner, companies that select individual point solutions for each regulatory challenge they face will spend ten times more on the IT portion of compliance projects than companies that take a more integrated approach. On the other hand, companies that implement an enterprise-wide, end-to-end automated compliance solution will not only be able to meet current and future compliance needs, they will also be able to increase efficiency and decrease costs.

To build an effective identity theft prevention program, Gartner recommends that institutions consider the following:

> Many organizations are rooted in manual processes because they are established and familiar. Be careful of saying, "This is how we have always done it."

- → Combine compliance requirements and implement synergistic solutions. This saves time and money, as well as establishes a framework for responding to future requirements.

- Monitor the total cost of compliance relative to its effectiveness. Higher spending will not necessarily mean a company realizes a higher level of compliance or better reduction of risk.
- Understand, categorize and communicate the risks of noncompliance to your business. Agree on your preferred risk profile.
- Create a "weather bureau" to forecast changes in governance and compliance requirements.
- Create an explicit link between compliance, performance management and value.
- Manage compliance as an ongoing program, not a project.
- Effective compliance requires organizational support, process control methodology and content control.
- To control compliance costs, look for commonality in compliance requirements, use an investment approach for budgeting and take complexity out of the system whenever possible.

Roadmap to Red Flag Compliance

In addition to the Gartner compliance recommendations, there are a number of steps that will help guide you to Red Flag compliance. Once red flags have been identified, a program should be incorporated and its documentation used to maintain and maximize compliance with FACTA Red Flag regulations. This documentation should include an overview of the risk assessment and Red Flags that were identified, along with solutions that were considered and justification of why solutions were or were not implemented.

Red Flag detection

An organization's internal staff members require training to maximize the detection rate and operational efficiency of Red Flag programs. This training acquaints staff members with key symptoms of identity theft, such as non-receipt statements or a customer's address change followed by a request for credit cards, checks or Personal Identification Number (PIN). Additional identity theft indicators include unexpected or uncharacteristic charges or collection of debt where the individual does not recognize the account.

An organization's customers should also be aware of steps they can take to prevent identity theft. For example, consumers should monitor accounts online and review credit reports at least once per year. They should install firewalls and anti-virus security; and go paperless to prevent mail from being taken. They should not provide account information over the phone, Internet, e-mail or text unless the consumer initiated contact. Promoting positive consumer behaviors will help reduce overall fraud losses while maximizing consumer satisfaction.

Appropriate response

When identity theft occurs, your response can determine a customer's experience with your organization. While negative responses result in customer attrition, decreased spending and damage to your brand image, positive responses lead to improved utilization, brand loyalty and ultimately, higher revenues.

Depending on the size of an organization, an individual or group may be appointed to assist customers who have been victims of identity theft. This proactive effort empowers an organization to track identity theft, build loyalty, build a strategic advantage over other competitors through consumer messaging and provide results for future risk assessments.

Each organization will have programs unique to their needs. Numerous existing programs, including Sarbanes-Oxley, Gramm-Leach-Bliley, the U.S. Patriot Act and PCI obligations can be incorporated into FACTA programs.

Periodic updates

To maintain Red Flag compliance, it is important to update your organization's identify theft procedures at regular annual, bi-annual, quarterly or monthly intervals. A tracking program allows administrators to measure overall success as well as determine timetables for scheduled reviews and which aspects of a program require updates.

The good news about Red Flag compliance is that many financial institutions don't need to recreate the wheel since many have processes and policies in place to comply with previous regulations. Efficient compliance involves developing internal procedures and controls, identifying high-risk areas and transactions, and creating employee training programs to remain up to date with changes in company policies and procedures.

With so much at stake, financial institutions cannot afford to go without an effective, automated identity fraud compliance solution. It is not a question of if identity fraud will happen to a customer; it's a matter of when.

Choosing Effective Identity Theft Solutions

Knowing the customer and effectively verifying information is critical to fraud detection and prevention programs. To effectively meet compliance needs and reduce fraud risks, companies should look to leading-edge risk and fraud prevention solutions that address the complex issues each business faces. The most effective theft prevention solutions help detect fraud in real-time and reduce identity theft—protecting a business' most valuable assets—its customer relationships and brand.

A wide range of identity theft prevention services and solutions are available for businesses of all sizes. From Red Flag consulting and training services that provide operational support for program implementations and optimize programs for Red Flag compliance, to application processing services that work in conjunction with bureaus to identify increased activity/inquiries and flag suspicious information for appropriate action, these solutions can help your organization reduce losses by recognizing red flags before they lead to default.

Identity theft solutions can provide protection for all of your business and customer data. Completely customizable solutions are available to avert identity theft and account takeover by authenticating account holders and quickly identifying risky applicants via direct access to an array of robust databases, including public and business records, phone records and credit bureaus.

There are also solutions that validate application data—including address, date of birth and Social Security number—and uncover alias names. In some cases, this maximizes application processing efficiency by providing immediate online access to more than 400 million consumer credit files.

In addition, there are Red Flag compliance solutions that verify the validity of change of address requests in existing covered accounts to satisfy the requirements of FACTA sections 114 and 315. This is accomplished by examining and segmenting fraud in address mismatch transactions through predictive analytics and technology that detects address changes that are "out of pattern." Automating this important function reduces manual review costs, verifies address changes immediately to improve responsiveness to cardholders and eliminates the need to develop an in-house solution.

Additional solutions are also available to decrease losses by identifying unusual activity and security breaches in real-time, delivering outbound digital messages with text-to-speech capabilities to capture customer responses at a fraction of the cost of using a live agent, and employing neural network cardholder profiling for authorization and transaction review. Each of these automated solutions reduces losses due to identity theft, increases efficiency and helps to ensure Red Flag compliance—all while boosting customer trust.

Seizing Opportunities with FACTA

Financial Institutions across the United States are faced with change and change isn't always easy. There are many things that need to be taken into consideration: internal politics, individuals personally invested in specific systems and processes, and issues surrounding job security. First Data has worked with banks of all sizes to review their operational areas and policies and to implement FACTA-compliant identity theft programs that span customer service, loan origination, collections and fraud. Here are a few examples of the challenges that First Data has solved for its customers:

Customer

Medium-sized regional bank with a 100-person customer service call center.

Problem

Account takeover identity theft was occurring frequently due to a lack of sophisticated authentication procedures. Customer contact centers are the first line of defense for account takeover identity theft prevention and asking for a customer's Social Security number and mother's maiden name is no longer adequate to verify someone's identity in many circumstances. Social engineering is becoming a pervasive problem as criminals become emboldened by the lack of authentication procedures for both over-the-phone and in-the-branch account updates.

Solution

In collaboration with First Data, the bank implemented a solution that empowers customer service agents to require additional authentication for specific account demographic changes or requests for new payment instruments. The online tool provides random questions that only the consumer can verify. The customer service agent does not have the answers, so they cannot lead the conversation. By using a tool that provides open-ended random questions, the average handle time of the call can be reduced while maintaining customer authentication.

Customer

Large national credit card issuer, processing over 500,000 loan applications per month.

Problem

Address discrepancies impacted approximately 20 percent of all the applications received. Some of the discrepancies could be settled with existing customer relationship data, but when the bank did not have an existing relationship with the consumer, the credit bureau information often did not match the application. Contact needed to be initiated with the applicant, and if contact could not be made, a letter requesting additional information and proof of address needed to be sent. The act of sending a letter for additional information decreased the likelihood of the loan being originated by 80 percent. Most applicants never responded to the request for information.

Solution

Origination processes have been simplified by automated batch processing of applications to screen addresses for potential high risk address discrepancies. If other regulatory "know your customer" validation is completed, and only the address needs to be verified, the process allows the bank to segment applications further. First Data helped the issuer develop a process to generate a risk score if the address is in a known fraud area or is at a high risk for fraud. If the risk score is high, then a manual review can be completed. If the score is low, the application is approved. The approval rate for loan origination is projected to increase, while fraudulent applications are identified faster.

Customer

Large national credit card issuer, processing collections through charge-off delinquency.

Problem

Approximately ten percent of the issuer's 30-day collectables was truly uncollectible debt. Identity theft, familiar fraud and first party fraud was mixed in with collectable debt, so collectors continued to attempt to contact the consumer. Valuable time was spent skip-tracing and attempting to contact the cardholder, with limited success. Collecting on fraudulent debt is more difficult and time-consuming than resolving true consumer delinquency, and the collectors had limited knowledge of how to collect the debt.

Solution

The issuer worked with First Data to identify fraud sitting in delinquency stages by segmenting collections into specific queues. Accounts with characteristics such as previously good payment history, returned mail and recent high card usage are queued separately, allowing collectors to conduct additional account research and focus on identifying the true consumer more quickly. Reducing efforts to collect on fraud in the early stages of delinquency saves operational time and costs months later. The skip tracing tool that collectors were using was identified as a Red Flag solution that could be used in other departments: loan origination, fraud and customer service can now use the same tool for cardholder verification in different circumstances. By sharing the same tool, operational costs were reduced and staff cross-training became simpler.

Customer

Regional bank on the East Coast with $2 million in annual revenue.

Problem

Identity theft hit this financial institution hard. Although cardholders were consistently told not to provide information in an e-mail, they did. Phishing incidents plagued the bank for months, with fraud decimating numerous existing cardholder accounts. Manual processes sought to identify the customers impacted, but the fraud was identified only when the customer called to advise the bank of transactions that were not valid.

Solution

Almost immediately a First Data solution was installed - a "smart system" or neural network - to identify customer spending patterns in conjunction with known fraud risks. Having the ability to decline authorizations that posed high risk immediately helped reduce the bank's fraud losses. Transactions are now reviewed when appropriate and customers are contacted to validate them, if necessary. It is impossible to stop phishing, and impossible to have every cardholder safeguard their information, but monitoring for potential fraud and declining when appropriate are helping to prevent account takeovers and identity theft.

What an Opportunity!

It's a given that identity thieves will think of new ways to exploit corporate systems. Whether it's check, over-the-counter, credit card, telephone or e-commerce fraud, criminals are always looking for new ways to beat the system—and financial institutions have to be ready to combat whatever comes at them. However challenging these may be, there are real opportunities for financial institutions to build and maintain their customer trust by promoting their commitment to preserving customers' assets and identities.

What makes the future look bright is that the majority of consumers believe financial companies can reduce identity theft. In a recent Unisys survey of U.S. consumers, 65 percent said they either somewhat agree or strongly agree that financial institutions can prevent identity theft. Of these same consumers, 78 percent also believe that it is the bank's responsibility to prevent attempted fraud before it occurs. Clearly, the pressure is on financial institutions to ensure that customer trust continues to grow.

With this responsibility comes hard work. Maintaining brand integrity is critical to building loyalty and ultimately revenues. The cost of compliance can be expensive and time consuming if it is not approached as a positive process for the organization. Manual procedures will hinder implemented programs by increasing costs and decreasing customer satisfaction.

Thankfully, there are automated, end-to-end fraud prevention and protection solutions available today to help companies increase consumer confidence while easing the transition to FACTA compliance. These range from credit and debit card fraud protection to customer strategic data management solutions. Financial organizations large and small would do well to look to technology solution leaders like First Data to help them achieve compliance and prevent identity fraud with the most cost effective and proven solutions.

Resources

Javelin Strategy & Research's 2008 Identity Fraud Survey Report,
http://www.idsafety.net/803.R_2008%20Identity%20Fraud%20Survey%20Report_Consumer%20Version.pdf

2008 Information Media Group Survey,
http://www.bankinfosecurity.com/whitepapers.php?wp_id=143

Identity Theft Assistance Center (ITAC),
http://www.identitytheftassistance.org/

Gartner, "Understanding the Costs of Compliance," July 7, 2006,
http://logic.stanford.edu/POEM/externalpapers/understanding_the_costs_of_c_138098.pdf

Unisys, Identity Theft Prevention and Detection: Are Your Branch Banking Customers at Risk?
http://www.unisys.com/eprise/main/admin/corporate/doc/Unisys_ID_Theft_Prevention_and_Detection.pdf

FTC 2007 Fraud Report,
http://www.ftc.gov/opa/2008/02/fraud.pdf

Fair and Accurate Credit Transactions Act of 2003 (FACTA),
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ159.108

First Data.

The Global Leader in Electronic Commerce

First Data powers the global economy by making it easy, fast and secure for people and businesses around the world to buy goods and services using virtually any form of payment. Serving millions of merchant locations and thousands of card issuers, we have the expertise and insight to help you accelerate your business. Put our intelligence to work for you.

As the global technology leader in information commerce, First Data helps businesses safely and efficiently comply with the ever-changing regulations affecting financial institutions and other organizations. This ensures that companies can cost-effectively manage compliance activities, gain greater insight into their operations, gain a competitive advantage, and build valuable consumer confidence in the company’s brand.

For more information on First Data’s fraud prevention and protection solutions, please visit http://www.firstdata.com/product_solutions/risk_management/fraud_prevention.htm

About The Authors

As Product Owner for Fraud and Risk Management Solutions for First Data, Krista Tedder is responsible for the development of fraud and collections solutions that meet the market challenges faced by financial institutions. During her three year tenure with First Data, Krista has led the STAR® fraud servicing team and managed the debit fraud call center. Prior to joining First Data, Krista spent five years with MBNA in various positions including fraud and risk management.

Glen Wordekemper, Vice President of Product Development for First Data, is responsible for identifying market challenges and industry trends, developing strategic products and solution sets to address those needs, and promoting solution sets to drive revenue growth in First Data’s current client base. Since joining First Data in 1991, Glen has served the company in leadership roles in product development for electronic commerce, customer correspondence, print/mail, loyalty and rewards, and client customer service.

For more information,contact your
First Data Sales Representative
or visit firstdata.com.