First Data

The Facts About FACTA

The Fair and Accurate Credit Transaction Act (FACTA) was signed into law on December 4, 2003. On January 1, 2008, the FACTA Red Flag Rules went into effect, requiring each financial institution or creditor to implement a written Identity Theft Prevention Program by November 1, 2008.

FACTA requires financial institutions and creditors to develop and implement a written identity theft prevention program to detect, prevent and mitigate identity theft. As a financial institution or creditor, you are ultimately responsible for complying with the final rules and guidelines even if you outsource an activity to a third-party provider.

Concerned About Your FACTA Compliance? First Data Can Help

Your goal as an organization is to meet fraud head on and exceed the privacy and security expectations of your customers. First Data offers a host of solutions designed to help your organization not only become compliant with the Red Flag Rule guidelines – but to help you stand apart from the competition as a leader in protecting consumer information from fraud and risk.

→ **Proven enterprise-scale fraud portfolio.** Our fraud products are already in use by thousands of credit and debit issuers across the U.S., including some of the largest in the world.

→ **Turnkey solutions.** You can incrementally add different capabilities offered by First Data, or expand your current use of First Data products and services. We offer a host of different combinations that can be tailored to compliment your identity theft prevention program and can be turned up quickly for any operation.

→ **Respond quickly to changing fraud and identify theft conditions.** First Data's Fraud Detection programs provide up-to-the-minute fraud strategies to better manage verification, allowing for increased approvals with high confidence of data accuracy

→ **An end-to-end solution.** Takes the guesswork and processing headaches out of the equation and allows you to focus on your customers and your business. First Data provides an end-to-end solution – from the verification of applicant data, to address changes, to out-of-pattern transaction recognition and throughout the consumer life cycle – improving profitability and increasing customer loyalty and satisfaction.

→ **Additional service offerings.** First Data is a global leader in fraud and analytics services with a wide-range of products and services that can be bundled together to provide a highly customized solution – from consumer data, to address information, consortium data and data analytics – that increases revenue and improves customer loyalty. In addition, First Data offers fraud and analytical consulting services via our Fraud Customer Operations group in order to provide you with some of the best services available in the industry.

First Data™

First Data FACTA Solutions

First Data provides superior information and analytics solutions to financial institutions, receivables management, auto finance and insurance industries. With the ability to instantly tap into millions of consumer, business and public records data, customers can verify information, authenticate consumers and businesses and investigate high-risk accounts. Our suite of hosted, predictive-modeling tools combines the power of analytics and information to generate actionable business decisions that reduce costs and increase productivity and overall profitability.

First Data Information Services

FACTA Compliance Issue: Fraud costs your business time and money. Now, FACTA Red Flag Rules require you to detect, prevent and mitigate identity theft to your covered accounts. The Solution: By helping you limit risks and reduce fraud, First Data helps strengthen your customer relationships and keeps your business growing strong. Our unique blend of experience, information processing and expert intelligence can help your business create efficient, long-term risk management strategies as well as short-term, day-to-day tactics.

→ **FastData℠ –** FastData can help you authenticate, verify, locate or identify individuals or businesses within seconds with access to the industry's largest and most accurate integrated information service. *For more information on FastData, click here.*

→ **SafeID Scores –** SafeID scores verify the validity of change-of-address requests and resolve address discrepancies.

→ **First Track® –** First Track is an advanced turnkey solution for today's case management processing needs. This remarkable system drives mainframe information straight to your desktop, where you can streamline all the tasks that currently slow you down. Information can be run against the First Track database in order to link known fraudulent activity. Application is only available to Omaha clients. *For more information on FirstTrack, click here.*

→ **FirstPursuit® –** FirstPursuit provides immediate online access to consumer credit information from both Equifax and TransUnion, two of the nation's leading consumer credit reporting agencies with access to over 400 million consumer credit files. FirstPursuit offers the flexibility to search a consumer's file with or without posting an inquiry. *For more information on FirstPursuit, click here*

→ **Fraud Detection Services –** Protect your profitability by stopping the growth of fraud activities - such as phishing, also known as spoofing and skimming - used to capture card and PIN information and create counterfeit cards. First Data now offers a new level of protection from these types of losses. With our solutions scoring for PIN-secured debit transactions, you can profile your cardholders' transaction activity to see a unified picture of their purchasing behavior. *For more information on Fraud Detection Services, click here.*

→ **Bureaus –** Bureaus can be used to identify increased activity/inquiries and to count the number of credit relationships with a number of recently opened accounts. Bureaus can report back to you on accounts that were closed for abuse and flag the account for the appropriate action. Bureaus can also be used to report new and recent activity on an account.

→ **First Data Fraud and Risk Consulting Service –** First Data also offers Fraud and Risk Consulting Services – providing you direct and immediate guidance on the usage of our products to reduce overall fraud and identity theft.

First Data

First Data Communications Services

FACTA Compliance Issue: You need to communicate with your customers and businesses about address changes, validation of questionable consumer data, additional plastic requests and other changes that occur on a daily basis to an account. And you need an automated and cost-effective solution to support this need. The Solution: First Data has several communication tools that can assist you in sending letters and postcards to consumers, contacting via telephone or providing VRU support, alert e-mails and other solutions.

→ **2Way-Connect℠ –** First Data's 2Way-Connect is an automated, interactive digital voice messaging solution with exceptional text-to-speech capability, allowing the delivery of messages tailored to a specific audience. With the ability to deliver both one- and two-way messages, customers can respond immediately if required, using voice or touch-tone options. Applications are wide and include many industries such as financial services, utilities, communications, government, insurance and healthcare. *For more information on 2Way-Connect, click here.*

→ **IVR –** Interactive Voice Response can be used to automate delivery of information at a time convenient for the consumer. IVR can also be used to provide disclosure or other repetitive information to ensure delivery of a consistent message.

→ **Live Agent –** Live Agent support can be used as a response mechanism for 2Way-Connect calls or for premium customers.

→ **Letters –** Letters can be generated for delivery of information at a time convenient for the consumer. This solution is especially useful when confirming changes in information such as address, phone number or name change. This solution is only available for Omaha based clients.

Additional Resources from First Data

→ **Client Training –** First Data Fraud Consultants can help maximize your Red Flag program by reviewing procedures and ensuring all aspects of the new regulations are covered.

→ **Application Processing –** First Data's application system, in conjunction with bureaus, can be used to identify increased activity/inquiries and to count the number of credit relationships with a number of recently opened accounts. First Data's application system receives the freeze from the bureaus and displays the information in First Data's application system for appropriate action.

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

Not all products are available on all platforms. Please check with your sales representative for specifications.

A 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.

First Data™

First Data FACTA Solutions At A Glance

First Data Solutions to assist Clients with their support of the Red Flag Rule Guidelines

Red Flag Rule Examples	Solutions Products	First Track	2Way-Connect℠	IVR/Live Agent	Bureaus	Letters	Apps Processing	Falcon	Adaptive Control	Reports	Training by Client
Alerts, Notifications or Warnings from a Consumer Reporting Agency											
1. A fraud or active duty alert is included with a consumer report.	●		●	●	●	●	●				
2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.	●		●	●	●	●	●				
3. A consumer reporting agency provides a notice of address discrepancy, as defined in § 41.82(b) of this part.	●		●	●	●	●	●				
4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:	●		●	●		●					
a. A recent and significant increase in the volume of inquiries;	●		●	●	●	●	●				
b. An unusual number of recently established credit relationships;	●		●	●	●	●	●				
c. A material change in the use of credit, especially with respect to recently established credit relationships; or	●		●	●	●	●	●				
d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.	●		●	●	●	●	●				
Suspicious Documents											
5. Documents provided for identification appear to have been altered or forged.											●
6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.											●
7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.											●
8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.											●

First Data™

First Data Solutions to assist Clients with their support of the Red Flag Rule Guidelines

Red Flag Rule Examples	Solutions Products	First Track	2Way-Connect℠	IVR/Live Agent	Bureaus	Letters	Apps Processing	Falcon	Adaptive Control	Reports	Training by Client
9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.											●
Suspicious Personal Identifying Information											
10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:	●						●				
a. The address does not match any address in the consumer report; or	●						●				
b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.	●						●				
11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.	●						●				
12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:	●	●			●						
a. The address on an application is the same as the address provided on a fraudulent application; or	●	●			●						
b. The phone number on an application is the same as the number provided on a fraudulent application.	●	●			●						
13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:	●										
a. The address on an application is fictitious, a mail drop, or a prison; or	●										
b. The phone number is invalid, or is associated with a pager or answering service.	●										
14. The SSN provided is the same as that submitted by other persons opening an account or other customers.	●				●		●				

First Data™

First Data Solutions to assist Clients with their support of the Red Flag Rule Guidelines

Red Flag Rule Examples	Solutions Products	First Track	2Way-Connect℠	IVR/Live Agent	Bureaus	Letters	Apps Processing	Falcon	Adaptive Control	Reports	Training by Client
15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.	●				●						
16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.			●	●		●	●				●
17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.											●
18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.	●		●	●		●					
Unusual Use of, or Suspicious Activity Related to, the Covered Account											
19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.	●		●	●		●		●		●	
20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud. For example:			●	●				●	●		
a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or			●	●				●	●		
b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.			●	●					●		
21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:			●	●				●	●		●
a. Nonpayment when there is no history of late or missed payments;			●	●					●		

First Data™

First Data Solutions to assist Clients with their support of the Red Flag Rule Guidelines

Red Flag Rule Examples	Solutions Products	First Track	2Way-Connect℠	IVR/Live Agent	Bureaus	Letters	Apps Processing	Falcon	Adaptive Control	Reports	Training by Client
b. A material increase in the use of available credit;			●	●					●		
c. A material change in purchasing or spending patterns;			●	●				●	●		
d. A material change in electronic fund transfer patterns in connection with a deposit account; or											●
e. A material change in telephone call patterns in connection with a cellular phone account.											
22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).			●	●		●		●	●		
23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.											●
24. The financial institution or creditor is notified that the customer is not receiving paper account statements.											●
25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.		●									●
Notice From Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Financial Institution or Creditor											
26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.		●									

The information above was derived in part from the Federal Register dated November 9, 2007, titled "Identify Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003; Final Rule." First Data makes no representation or warranty as to the accuracy or completeness of any information above. Product options may not be available on all platforms.