SEARCHFINANCIALSECURITY.COM

technical guide on

RED FLAG RULES COMPLIANCE

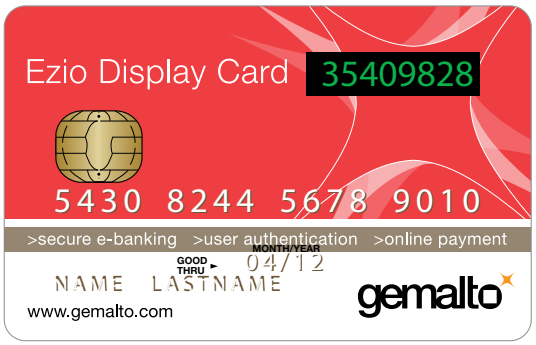
contents

TechTarget
Where Serious Technology Buyers Decide

Gemalto Ezio authentication solutions for online banking

By providing end-to-end services and comprehensive solutions, Gemalto helps financial institutions introduce strong authentication solutions that protect personal identity information and guard against cyber crime.

- > Strong authentication solutions serving 10 million users worldwide
- > High assurance Online Banking security
- > Highest compatibility within all industry standards



www.gemalto.com

gemalto
security to be free

insight

Red Flag Rules

Two years ago, the Federal Trade Commission decided to stem the tide of rampant fraud and identity theft by instituting the Red Flag Rules. Financial services organizations must comply with the rules or face heavy penalties and possible civil action.

SEARCHFINANCIALSECURITY.COM presents a comprehensive guide to Red Flag Rules compliance. Our experts cover all the angles with authoritative technical advice on: using a risk-based approach for compliance; specific examples of red flags; clarification of the guidance; and what industry organizations are doing to help victims.

contents

RISK MANAGEMENT

Red Flag Rules Compliance Demands A Risk-Based Approach

Organizations are challenged to assess, monitor, mitigate and manage risk of suspicious behavior that indicates possible identity theft. BY MICHAEL RASMUSSEN

FINANCIAL-SERVICES FIRMS, as well as organizations in other industries, face significant risk if they cannot demonstrate compliance to the federal Red Flag Rules. The Red Flag Rules stem from the implementation of the Fair Credit Reporting Act and aim at reducing the threat of identity theft. An alarming number of organizations are unaware of the liability they face for non-compliance.

Some organizations are willing to sit back and see how the Red Flag Rules are enforced since they are not a "policed" regulation. Regulators are not going to send out their compliance cops to see if organizations are compliant on a proactive basis; neither the FTC nor the financial regulators have any active plans to proactively audit organizations. Rather, the regulation is reactive in that it invokes an investigation and liability when an incident occurs. This may come in the form of a data breach or an internal whistle blower notifying authorities or the public of an incident. Companies that have a violation of non-compliance face monetary penalties and potential civil litigation. The most significant risk comes from civil liability where an individual can sue the corporation for actual damages from an identity theft breach; this also allows a class-action suit.

Companies that have a violation of non-compliance face both monetary penalties and potential civil litigation.

Red flags are aimed to protect individuals from identity theft by assuring that organizations that collect sensitive financial and personal information are actively monitoring the risk of identity theft. The rules offer 26 key risk indicators (KRI) of suspicious behavior that are guidelines, but not an exhaustive list for organizations to actively monitor. KRIs include altered documents, fraud alerts on credit reports, unusual account activity, and suspicious address changes.

Compliance with the Red Flag rules must take a risk-based approach. Organizations are not given a specific set of items to implement; there is no detailed checklist. Compliance is principle-based focused on the outcome—avoiding identity theft—

and not on specific requirements. The organization is challenged to assess, monitor, mitigate and manage risk of suspicious behavior—red flags—that indicate possible identity theft. At a high-level, compliance involves:

A compliance program. Organizations need to implement a program that effectively detects, prevents and mitigates identify theft risk. This is effectively a risk-based process that identifies where identity theft may occur, assesses the significance of this risk, implements controls to mitigate risk to acceptable levels, and monitors corresponding KRIs to alert on suspicious behavior.

Oversight. The program needs to be managed on a continual basis by somebody who is accountable for its operation; for some organizations this may be a chief compliance officer, while in others it will fall to the CISO. Oversight of the program is essential with clear lines or reporting to executives and the Board of Directors. As identity theft risk involves multiple areas and functions within the organization, the oversight role needs to build a collaborative effort to manage risk and compliance across legal, corporate compliance, information security, physical security, privacy, enterprise/operational risk management and records management.

An organization must implement and maintain clear and current policies and procedures that instruct individuals on how to protect and manage the security of sensitive identity information.

Policies & procedures. An organization must implement and maintain clear and current policies and procedures that instruct individuals on how to protect and manage the security of sensitive identity information. This is fundamental to any compliance program and provides the foundation of what organizational expectations are for behavior and control. Policies and procedures are to have a single owner responsible for their development and maintenance, but be written collaboratively with all responsible parties. Every policy should be reviewed at least annually to validate that it is still appropriate and effective to maintain compliance and manage risk. Policies that are outdated or which put the organization in a state of non-compliance must be addressed immediately

Training. Publishing policies and procedures alone are not enough; Organizations need to demonstrate that employees and business partners are adequately trained on compliance as well as to defined policies and procedures What courts and regulators expect is that organizations go above beyond simple publication and availability of policies to demonstrating that individuals are trained and understand what is expected of them. Red Flag Rules compliance will have an ongoing training program in either a classroom or e-learning environment to train employees and business partners.

Risk assessment. Organizations need to be continually monitoring for risk of identity theft. At its base, this involves making sure people are who they say they are; authenticating identities is critical. A risk assessment is best done according to standardized methodologies. The best risk management/assessment process methodology is found in the draft of ISO 31000 (which is built on the AS/NZS 4360:2004 Risk Management Standard). This methodology takes an organization through the risk

management and assessment process and is easily adaptable to managing risk around identity theft and maintaining compliance.

Audit compliance. Red Flag rules compliance requires regular validation of the program, policies, procedures, training and overall effectiveness of compliance. A cooperative effort should be in place between management responsible for Red Flag Rules compliance and the internal audit function, and a regular audit schedule and work paper plan should be implemented to monitor the effectiveness of the compliance program.

Investigations. A good risk management program for Red Flag Rules compliance will also have an integrated investigations process that helps the organization manage identity theft incidents. Each incident should be documented and loss to the organization should be measured. Loss metrics and data are fed into the risk assessment process to help the organization learn from incidents and calculate exposure based on the history of events.

Michael Rasmussen, a governance, risk and compliance (GRC) expert, is with Corporate Integrity, LLC. He is a keynote speaker, author and collaborator on GRC issues around the world and is noted for being the first analyst to define and model the GRC market for technology and professional services. Corporate Integrity, LLC is a strategy & research advisory firm providing education, research and analysis on enterprise governance, risk management and compliance.

GOVERNANCE

FACTA's Red Flags of Identity Theft

Learn how car dealerships to debt collectors need to adjust to comply with FACTA's Red Flag Rules. BY ROBERT MULLINS

TWO YEARS AGO, new Federal Trade Commission (FTC) rules went into effect requiring businesses to recognize the "red flags" that tell them someone may be committing fraud.

Businesses that maintain personal financial information on customers—from banks to auto dealers—must now have systems in place to spot red flags and intervene to stop a possible identity theft.

"If someone were to apply for credit and they put down their date of birth and then a Social Security number that does not correlate to the date of birth, that would be a red flag," said Paul Metrey, director of regulatory affairs for the National Auto Dealers Association (NADA), which hosts data security workshops for dealers.

The Red Flag rules from the Federal Trade Commission (FTC), which took effect Nov. 1, 2008, are a follow-up to the Fair and Accurate Credit Transactions Act (FACTA) enacted in 2003. FACTA requires businesses to have systems in place to secure the personal financial information of customers and to securely dispose of that information when it's no longer needed.

Besides auto dealers, businesses subject to FACTA include debt collectors, mortgage brokers and even someone who obtains a credit report on a prospective nanny, according to the FTC.

RED FLAGS

The following are examples of red flags, according to the FTC:

- **The majority of available credit on a card is used for cash advances or merchandise that is easily convertible to cash, such as jewelry;**
- **A noticeable change in electronic fund transfer patterns on a deposit account;**
- **Purchases in two distant cities on the same day;**
- **Identification documents provided to open an account appear to have been altered or forged;**
- **Customer can't answer challenge questions such as identifying their mother's maiden name.**

"Whether someone hiring a nanny is aware [of FACTA], I don't think there are, obviously. But I think financial institutions are aware of it and they have to be," said Mary Monahan, senior analyst with Javelin Strategy & Research, which focuses on the financial services industry.

Keeping dealerships secure

Car dealers regularly work with finance companies, but there is no one data security plan for all of them, said NADA's Metrey. "The procedures you adopt should be appropriately tailored to the size and complexity of your operation."

For a small dealer, selling just a few cars per month, security could be as simple as advising the finance manager not to leave contracts on their desk when they leave the office.

For a large dealer group with multiple car maker franchises, though, best practices include password-protected access to servers only for people whose job descriptions entitle them access. A service department manager can access a customer's vehicle maintenance records, but not their finance records. Servers should be in a secure, climate-controlled room and not accessible via the Internet, NADA advises in a guide to dealers.

"The procedures you adopt should be appropriately tailored to the size and complexity of your operation."

–PAUL METREY, director of regulatory affairs, National Auto Dealers Association (NADA)

Don't reinvent the wheel

Privacy regulations have been imposed on debt collectors for years, so new rules such as FACTA aren't all that new to them, said Leslie Bender, an attorney specializing in privacy laws who represents a debt collection industry group.

Debt collectors, who obtain personal financial records of debtors to collect money on behalf of client creditors, have been subject to the Fair Debt Collection Practices Act for about 30 years. They and vendors of computers, firewalls or document shredding services, are "light years ahead" of other industries on their security policies, said Bender.

"Debt collectors are attuned to protecting consumer data and don't just pitch it into the dumpster," she said.

But besides securing and properly disposing of records, financial institutions now also have to be further diligent under the Red Flag rules.

Robert Mullins is a reporter covering the technology industry from Silicon Valley. He writes about servers, storage, security, open source software and other topics.

COMPLIANCE PROCESSES

How Financials Prepared for Red Flag Deadline

Compliance with federal requirement for ID theft prevention program required credit union to unify policies.

BY MARCIA SAVAGE

For Star One Credit Union, which serves some 76,000 members in the heart of Silicon Valley, complying with federal Red Flag rules requires a lot of policy coordination and documentation.

"We have a lot of the pieces in place under current policy and procedure," said Lynn Brubaker, vice president of deposit services at Star One. "But Red Flags is requiring that we bring it all together under one policy and cross reference all those policies and procedures so that at a glance, an examiner or anyone could see what we're doing to mitigate ID theft," Brubaker said.

Once all the policies are coordinated, it will be a matter of training staffers, such as a teller, on how to spot a red flag, she said. Training will need to be job specific and ongoing, she added.

The Red Flag rules, issued by the Federal Trade Commission and federal banking regulators last October, took effect Jan. 1, 2008. They require financial institutions and creditors to have policies and procedures for spotting red flags that indicate possible identity theft, and systems for thwarting the crime in connection with new and existing accounts. The regulations implement Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003. Organizations had to be in compliance by Nov. 1, 2008.

For many financial institutions, compliance with the rules may be more about documentation of existing procedures—as in Star One's case—rather than starting from scratch. A Gartner survey of 50 U.S. banks conducted in March and released in May, showed that banks are spending more on fraud prevention this year, but not because of the Red Flag regulations. Sixty percent of the banks surveyed believe they're already compliant with the rules.

"The intent is to protect consumers from identity theft, but it probably just requires some fine tuning, not a major overhaul of what they're doing today in most cases."

–AVIVAH LITAN, vice president and distinguished analyst, Gartner

"The intent is to protect consumers from identity theft, but it probably just requires some fine tuning, not a major overhaul of what they're doing today in most cases," said Avivah Litan, vice president and distinguished analyst at Gartner.

"It depends on how important fraud is to an institution," she added. "Some of the large banks are taking this very seriously and looking at it as an opportunity to beef up their multichannel, crosschannel strategies."

Craig Priess, vice president of marketing at Guardian Analytics, a supplier of online fraud prevention technology, said his company is getting a lot of questions about the Red Flag rules from financial institutions.

"It's definitely on the radar," he said, but added that the regulations aren't getting the same amount of attention as the Federal Financial Institutions Examination Council (FFIEC) guidelines for strong authentication.

In general, the regulations don't pose a huge problem for large financial institutions, said Jonathan Gossels, president and CEO of security consulting firm SystemExperts.

"What we're seeing is, it has to do with the size of an organization. Larger ones were moving down that path anyway. They're used to complying with regulations," he said. "Smaller organizations are always resource constrained, so any new regulation is a burden."

The FTC offers 26 examples of red flags that financial institutions and creditors can consider including in their identity theft prevention programs. They include: personal information provided by the customer isn't consistent with other personal data provided by the customer; an account is used in a way that is inconsistent with established activity patterns; and shortly after notice of a change of address, an institution receives a request for new or additional cards.

"There isn't a defined set of red flags," Gossels said. "They're characteristics that an organization is supposed to develop to set up their red flags."

Compliance with the regulations is fundamentally about policies and procedures, but some technology can help, he added.

At Star One, the Guardian Analytics technology it implemented to secure its online channel will be a tool used in its overall Red Flags policy, said Margarete Mucker, vice president of remote services. Online banking is popular among its members, who are mostly high-tech workers.

Brubaker said compliance will be an ongoing activity. "This is obviously a living, breathing document," she said.

The credit union, which has assets of more than $3.5 billion, is performing its policy work manually, but is planning to implement software that will help automate the process, Brubaker said.

Gossels noted that the Red Flag rules affect more than financial institutions. They also impact businesses such as auto dealers, utility companies and telecommunications companies.

Auto dealers and smaller organizations will struggle with the rules, Gossels said. "Car dealers don't want to be in a position to deal with credit and reporting on discrepancies with addresses. That's not their business."

Litan also said non-banking businesses will be hit the hardest by the rules, but noted that there aren't enough FTC examiners to check their compliance.

The FTC doesn't "have the staff to examine all these companies and most of them don't have anything in place," she said.

Marcia Savage is editor of SearchFinancialSecurity.com.

Q&A WITH MARK STEINHOFF

Red Flags Rule: Unclear Guidance Biggest Challenge

Maintain compliance with the Federal Trade Commission's Red Flag regulation for financial institutions.

BY MARCIA SAVAGE

Red Flag Rules, issued by the Federal Trade Commission and federal banking regulators took effect Jan. 1, 2008. It requires financial institutions and creditors to have policies and procedures for spotting red flags that indicate possible identity theft, and systems for thwarting the crime in connection with new and existing accounts. The regulation implements Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003. SearchFinancialSecurity.com asked Mark Steinhoff, national financial services lead and principal at Deloitte & Touche LLP's security and privacy services, for insight into the rule and how organizations can handle the new requirements.

SEARCHFINANCIALSECURITY.COM: Let's start with an overview of the Red Flag regulation. What do financial institutions need to do to maintain compliance?

Mark Steinhoff: The provisions require organizations to develop and implement a written identity theft prevention program that would be approved by an appropriate senior-level management committee. It's supposed to be a program that would also include various components reflecting the appropriate governance structure as well as how the program would be administered on a continuing basis; it should also address policies and procedures around the identity theft program. This obviously incorporates the risk assessment process: an organization would need to identify the types of covered accounts that are described in the rule. The company would also need to reflect, for example, how it has looked at its service provider community and its policies concerning ongoing training and awareness internally as well as for customers. Finally, there's a requirement to report on the effectiveness of the program…. The rule also mentions that this program should be a standalone program, not necessarily confused with or buried in existing anti-money laundering processes.

SEARCHFINANCIALSECURITY.COM: Financial security managers have said they were already doing a lot of what the Red Flag regulation requires, but the challenge is documentation.

What advice do you have for them?

Mark Steinhoff: An effective approach is first to understand what aspects of the rule—and the red flags that are listed in the rule—actually apply to the organization, and then understand what practices are already in place in the organization that address them. While the rule indicates that it should be a standalone program, it's not clear what the definition of standalone program is.

One of the challenges many of our clients have is the competing compliance requirements. While the program may need to be to initially established as a standalone, that doesn't mean it can't be integrated with other practices. Once you understand what you're doing today, there's a challenge around documentation…. you have to document that you have "a written program." The guidance doesn't necessarily tell you what that should look like or how extensive those policies and procedures should be, but it's important there should be documentation around the risk assessment process. One of the things the regulators always look at is the process you went through to determine your risk levels and how you're going to mitigate those. There are other challenges around documenting what you're doing to provide ongoing training and awareness, and ultimately deciding what the right level of reporting that's required at what levels of management is… There is really documentation at two levels: first, documenting how you went through the risk-assessment process and, second, documenting the practices that will be in place to mitigate risk going forward.

SEARCHFINANCIALSECURITY.COM: Can you elaborate on the training requirements?

Mark Steinhoff: Training should be looked at on two levels. One is general training and awareness for the mass of employees and customers around the program itself: Why are we doing this, what's required of us, and what are we doing on an ongoing basis? The next level down would be to understand how the training relates to specific red flags.

The training and awareness around the specific red flags should be tailored to a particular practice at the organization. For example, most organizations have an existing third-party or service provider risk assessment process. They would need to update their policies and procedures to make sure they incorporated attention to the appropriate red flags for those service providers who are involved in either the processing or collection of data in covered accounts. Individuals who are executing those procedures would need to be aware of that program and how the results need to be reported.

SEARCHFINANCIALSECURITY.COM: Are financial institutions aware that the Red Flag provisions incorporate requirements for service providers?

Mark Steinhoff: It's one aspect of the Red Flag rules that is not necessarily highlighted but it's referenced and noted that institutions need to address this. Again, there's no firm guidance on how to go about doing it. Third-party service providers and business partners [that handle information in covered accounts] are probably one of the biggest risks related to privacy, data protection and identity theft. It's been important for us to make them [clients] aware of how important that component is to their overall program.

SEARCHFINANCIALSECURITY.COM: What are your recommendations for ongoing compliance?

Mark Steinhoff: Our recommendation would be to address the specific provisions of the rule by looking at them in light of existing risk management and compliance initiatives as they relate to data protection, identity theft and privacy and anti-money laundering and customer identification programs, to ensure there is a holistic view. Oftentimes, we've seen that organizations will create a new program—maybe in one part of the business or selected parts of the business—without a holistic view, particularly as it relates to governance and oversight as well risk assessment. While the rules are requiring institutions to make sure this is a standalone program…this is very much an issue around protection of data. So integrating this with existing programs will allow institutions to address these issues on an ongoing, sustainable basis as opposed to creating something that's more onerous than it needs to be.

SEARCHFINANCIALSECURITY.COM: Will the upheaval in the financial services industry affect compliance efforts?

Mark Steinhoff: In the short term, all of these events clearly are a distraction from the day-to-day plans and practices. The longer term implications are continued competition for time, money and resources to address these issues. I don't believe the regulators are going to allow organizations to use the current market conditions as an excuse for not addressing these requirements. [Market conditions] make it that much more important to integrate this with existing practices. There's already tremendous pressure on organizations around fraud, identity theft, and data protection; this is just adding to it. Over the last eight to 12 months, the regulators have raised the bar relative to practices in these areas…it's not sufficient to have policies and procedures; they want to know more about where the data is, how you are protecting it, and how you are protecting your customers and employees.

Marcia Savage is editor of SearchFinancialSecurity.com.

Q&A WITH ANNE WALLACE

Identity Theft Assistance Center Marks Five Years of Helping Victims

Head of Identity Theft Assistance Center talks about how the center helps Red Flag Rules compliance.

BY MARCIA SAVAGE

The Identity Theft Assistance Center (ITAC), a nonprofit cooperative of financial-services companies, is celebrating its fifth anniversary with a reception in Washington, D.C. on Wednesday. ITAC has helped 60,000 of its 38 member companies' customers recover from identity theft. SearchFinancialSecurity.com recently met with ITAC President Anne Wallace to discuss ITAC's work, identity theft investigations, and the Red Flags Rule.

SEARCHFINANCIALSECURITY.COM: What does the Identity Theft Assistance Center do?

Anne Wallace: ITAC is a cooperative initiative of the financial-services industry. About six years ago, 50 of the largest financial-services companies decided if they worked together, they could do a better job at helping their customers recover from identity theft and detect fraud as part of that process. So they formed a nonprofit membership corporation, owned and managed by the members.

The basic concept is that identity theft typically doesn't just affect one company; it affects multiple companies and the consumer is groping around in the dark trying to find out where fraud has occurred. ITAC reduces that frustration and the time lag in helping the consumer find out where else the bad guys have struck. We also hold people's hands and walk them through the process; they talk to a real live person who is knowledgeable and sympathetic and can make them feel like someone cares and they really are in control. This is a free service for the consumer, paid by the member company.

That's primarily what we do, but behind that is also a fraud detection service. As part of this victim assistance service, the consumer will be walked through their credit report. A consumer might say, "I don't recognize that account." We notify all those companies of what may be fraud. The whole idea is that kind of fast notice allows our members to find fraud across their organizations. If the consumer spots suspicious activity at a company that's not a member, we notify them too: a retailer, a telecom—anyone who

shows up in a credit report. The final part of the mission is to share data with law enforcement. We've gotten the consumers' consent to this as part of our privacy policy.

SEARCHFINANCIALSECURITY.COM: What trends are you seeing this year in fraud and identity theft?

Anne Wallace: From the victim's side, it's the same schemes we've seen historically. We typically ask consumers if they know how the fraud occurred and in most cases they don't. Of those who do know, we ask how they believe it happened. It's the same causes: lost or stolen wallets, some hacking. Those patterns of lost information, hacking, friends or family, and household fraud really haven't changed much…We know the FBI and others are very concerned about international gangs and crime rings, but the victim doesn't typically know [about] that.

SEARCHFINANCIALSECURITY.COM: Have there been any advancements in identity theft investigations? Is there any more success with prosecution?

Anne Wallace: The anecdotal information is they're [law enforcement] paying a lot more attention. There's been an enormous change in last five years in terms of recognition of the seriousness of this crime, not just because of the impact on the individual…Particularly after 911, there's the recognition that identity theft is a facilitator of a lot of other and more serious crimes…human trafficking, terrorism. It is a characteristic, or a part of many serious crimes, both economic and violent.

A big change has been these task forces that are organized in a lot of cities; most are headed by the U.S. Postal Inspection Service and the FBI. They're bringing together the federal agencies and state and local agencies. They're phenomenally successful. If you have an immigration problem, the crime looks very different to a police officer than it does to an FBI agent. They'll see different aspects of the crime. These task forces have been very successful in getting past the biggest hurdles in identity theft investigations, which are jurisdictional…If you can have multiple victims and higher dollar losses, suddenly the prosecution may become a lot easier.

SEARCHFINANCIALSECURITY.COM: Have you seen any impact yet from the Red Flags Rule in preventing ID theft?

Anne Wallace: Not really from a consumer standpoint. From an institutional standpoint, many financial institutions had investigative processes but they may not have been integrated across the institution. They often weren't. The thing about Red Flags is it forces an enterprise-wide review of what's this unit doing, what that unit's doing. So on one level, it's just compliance. But the substance is that it's the integration and consistency across the enterprise

SEARCHFINANCIALSECURITY.COM: What role does ITAC play in financial institutions' identity theft prevention programs?

Anne Wallace: Our members are saying that it's a big part of what they talk about in their compliance plan on the detection side—the reports ITAC sends our members is

the information they use to detect suspicious activity. It's also part of compliance on the back end; now that you know someone is a victim, what do you do? It goes back to this question of enterprise-wide awareness. What I hear from my members is they had an advantage in approaching Red Flags because the essence of ITAC is a single point of contact and an enterprise-wide approach to this. The whole idea of ITAC is no matter what unit of the bank deals with the consumer—whether it's student lending, mortgages or personal loans—all of those individuals should be offered the opportunity to use ITAC and you must have a mechanism for giving them the chance to use the service.

SEARCHFINANCIALSECURITY.COM: How can financial institutions become members of the Identity Theft Assistance Center?

Anne Wallace: We're looking for ways to do that. We recognize there's a need for a lot of companies to use ITAC and we'd love to find ways through other trade associations or the card associations to make ITAC available, particularly to smaller companies. They may not have a huge volume, so it's not like it would be a regular thing but if they do have a need, we want to make it available. We've been looking for other channels so we can serve more companies.

Marcia Savage is editor of SearchFinancialSecurity.com.

TECHTARGET SECURITY MEDIA GROUP

SearchFinancialSecurity.com

EDITORIAL DIRECTOR Michael S. Mimoso

SEARCHFINANCIALSECURITY.COM
SENIOR SITE EDITOR Eric Parizo

NEWS DIRECTOR Robert Westervelt

ASSISTANT EDITOR Maggie Sullivan

ASSOCIATE EDITOR Carolyn Gibney

ASSISTANT EDITOR Greg Smith

ART & DESIGN
CREATIVE DIRECTOR Maureen Joyce

VICE PRESIDENT/GROUP PUBLISHER
Doug Olender

PUBLISHER Josh Garland

DIRECTOR OF PRODUCT MANAGEMENT
Susan Shaver

DIRECTOR OF MARKETING Nick Dowd

SALES DIRECTOR Dara Such

CIRCULATION MANAGER Kate Sullivan

ASSOCIATE PROJECT MANAGER
Allyson Kinch

PRODUCT MANAGEMENT & MARKETING
Corey Strader, Andrew McHugh, Karina Rousseau

SALES REPRESENTATIVES
Eric Belcher ebelcher@techtarget.com

Patrick Eichmann peichmann@techtarget.com

Jason Olson jolson@techtarget.com

Jeff Tonello jtonello@techtarget.com

Nikki Wise nwise@techtarget.com

TECHTARGET INC.
CHIEF EXECUTIVE OFFICER Greg Strakosch

PRESIDENT Don Hawk

EXECUTIVE VICE PRESIDENT Kevin Beam

CHIEF FINANCIAL OFFICER Jeff Wakely

EUROPEAN DISTRIBUTION
Parkway Gordon Phone 44-1491-875-386
www.parkway.co.uk

LIST RENTAL SERVICES
Julie Brown
Phone 781-657-1336 Fax 781-657-1100

TechTarget
Where Serious Technology Buyers Decide

"Technical Guide on Red Flag Rules Compliance" is published by TechTarget, 275 Grove Street, Newton, MA 02466 U.S.A.; Toll-Free 888-274-4111; Phone 617-431-9200; Fax 617-431-9201.

SPONSOR RESOURCES

Gemalto

See ad page **2**

- Online Banking Products
- Gemalto Consulting Services
- The World Leader In Digital Security

About Gemalto

In a world where the digital revolution is increasingly transforming our lives, Gemalto's end-to-end security solutions are designed to make personal digital interactions more convenient, safe and enjoyable.

Our activities range from the development of software applications through the design and production of secure personal devices such as smart cards, SIMs, e-passports and tokens, to the deployment of managed services for our customers.

More than 1 billion people worldwide use our products and services for telecommunications, financial services, e-government, identity and access management, multimedia content, digital rights management, IT security, mass transit and many other applications.

As the use of Gemalto's software and secure devices increases with the number of people interacting in the digital and wireless world, the company is poised to thrive over the coming years.