

# PREPAID NAVIGATOR

## FAQs on Compromised Cards

### What is a compromised card?

A compromised card is a card that is at risk of being used fraudulently. Cards may have been compromised due to computer theft, unauthorized network intrusion, or any other types of suspicious activity (i.e. phishing e-mails).

### How does Sunrise Banks react to compromised notifications?

Sunrise Banks takes every compromised notification seriously and may require the issuance of new cards for affected programs. Program Managers will receive an e-mail notification if their card data has been compromised which will list the impacted account numbers.

### When notified about a card compromise, do all Program Managers block and reissue cards?

No. Some Program Managers do not reissue cards, or notify their customers of a compromise. Instead, they may monitor the account activity, and if there are any signs of fraud, take the appropriate action at that time; however, you need to evaluate the risk to your program and take the appropriate steps you feel necessary. Remember, most compromises involve the card number, expiration date and other sensitive card information.

Fraudulent activity may occur if your cards are not blocked and it could occur days, weeks, months or even years from now. The fraud dispute process can be inconvenient and cumbersome. While many customers do not experience fraud when a compromise is reported, the risk exposure still exists if the cards are not blocked and replaced. To protect your customers, minimize inconvenience and losses, Sunrise Banks strongly urges that all compromised cards be replaced.

### What information can be relayed to a cardholder about the compromise?

The name of the merchant or processor where the breach occurred is rarely released by MasterCard or Visa. In very large breaches which affect millions of cardholders, the name is usually made known to cardholders through the press. Since the specific information regarding the compromise is not released with the notice, if you decide that your accounts should be closed and replaced, we would advise you to only inform the cardholder that you received notice that their card was involved in a compromise and that you were not provided with specific details, but it's in their best interest to close their account and issue them a new card.

## VISA Automated Fuel Dispenser Liability Limit

Visa has announced revised standards for chargeback processing of Automated Fuel Dispenser (AFD) transactions in the U.S. region.

Effective April 15, 2015, Visa will increase the chargeback protection amount at Automated Fuel Dispensers in the U.S. Region from \$75.00 to \$100.00 USD, or the equivalent in the BIN issuing currency.

The impact of the change is an increased risk for negative balances. The new recommended limit for AFDs is \$99.00 USD or the equivalent in the issuing currency.



# Compliance Considerations

## Annual Notification Requirement Reminder:

Annual Error Resolution and Privacy Notices, to the extent applicable for each respective Program Manager, need to be sent annually to all active card accounts. Sunrise Banks defines an active account as any account that has had customer initiated transaction activity within the last 12 calendar months. You should already be in receipt of the 2014 Sunrise Banks Prepaid Card Privacy Notice Safe Harbor Format Template and the 2014 Sunrise Banks Prepaid Card Annual Error Resolution Notice Template. The notices must be delivered to cardholders by December 15th 2014. You are responsible for providing documentation to Sunrise that demonstrates:

- a. That all active accounts have received the Notifications (e.g. receipt of mailing);
- b. The method delivery (e.g. US Postal Mail) - this typically is done by working with your processor;
- c. The Date of delivery; and
- d. A copy of the Notice that was provided.

You are required to provide Sunrise with reports/evidence of delivery by 12/31/2014 via email (secure email if the documentation provided contains any Non-Public Personal Information) to prepaidcompliancegroup@sunrisebanks.com CC: Tyler.Seydel@sunrisebanks.com and the Relationship Manager servicing your account.

## Regulation E Reminders:

Federal ACH payments are allowed to prepaid cards provided the prepaid card complies with all requirements, and provides the cardholder with all the consumer protections that apply to payroll card accounts under Regulation E ("Reg. E"). Sunrise Banks requires all General Purpose Reloadable cards or any Card with direct deposit/ACH functionality comply with the Payroll Card provisions of Reg. E.

Reg. E outlines the communication requirements as well as the timeframes for investigating and resolving errors. Responses to Consumer disputes must be within the timeframes requested in Reg. E.

When a Program Manager receives a consumer dispute, they must investigate, resolve and provide written responses within the required timeframes as outlined in Regulation E. Program Managers are also obligated to complete and return the requested Sunrise Banks Transaction Dispute Log every month. These Dispute Logs are created by the Program Manager to identify and track all disputes.

## Regulation E Continued Oversight/Audit Notification

As a Program Manager you may be aware, or in receipt of, a Regulation E Transaction Dispute Compliance Review Request. These Requests are being sent out monthly in order to ensure proper oversight and performance of the dispute/provisional crediting process. This monthly review schedule will be adjusted once a Program Manager has had a few "clean" reviews (i.e. no Reg. E related issues as they pertain to the handling of an account with a transaction dispute), at that time we will scale back our level of oversight and move each Program Manager to a more appropriate review schedule commensurate with their performance, such as quarterly or semi-annually. Until such time that your review schedule has been adjusted your continued attention to the Requests is appreciated.

## Social Media Guidance:

The use of social media by a Program Manager to attract and interact with customers can impact their risk profile. The increased risks can include the risk of harm to consumers, compliance and legal risk, operational risk, and reputation risk.

# Compliance Considerations (continued)

The *Sunrise Banks Prepaid Card Product Social Media Standards Guide* is currently being finalized and will complement the *Sunrise Banks Prepaid Collateral Review Guide* (if you are unable to find your copy or feel you would like an additional copy please contact your Relationship Manager). The standards set forth in the *Sunrise Banks Prepaid Collateral Review Guide* apply to social media marketing collateral and the new guidance will walk through unique social media considerations and the compliance and legal risks associated with this marketing channel; it will also outline Sunrise Banks social media channel requirements, as well as what Sunrise Banks expects to be contained in the Program Manager's Social Media Management Program – to the extent a Program Manager is using social media – defined as a form of interactive, online communication in which users can generate and share content through text, images, audio and/or video.

## **Reminder – MasterCard Revised Standards: Limitation of Liability of Cardholders for Unauthorized Use (“Zero Liability”)**

MasterCard is revising its “Zero Liability” rule in the U.S. region by simplifying the language and applying the rule to all MasterCard® branded POS and ATM transactions.

Rule 6.3—Limitation of Liability of Cardholders for Unauthorized Use of Chapter 14, United States Region, of the MasterCard Rules, limits a MasterCard cardholder's liability for an unauthorized transaction.

### **The following revisions to the rule were effective 17 October 2014:**

- i. The rule will apply to all transactions conducted with a MasterCard® branded card, including PIN-based transactions at the POS and ATM.
- ii. A cardholder will not be liable for an unauthorized transaction, as long as the cardholder has exercised reasonable care in safeguarding the card from risk of loss or theft, and, upon becoming aware, promptly reporting the loss or theft to the Program Manager.
- iii. The rule will continue to apply to cards issued for small business programs, but not to other commercial cards. In the case of a prepaid card, the rule applies once the cardholder's identity has been registered with the Program Manager.

### **The following applies with respect to United States Region MasterCard Cardholders.**

A Program Manager cannot hold a Cardholder liable for a Transaction that was not authorized by the Cardholder if the Cardholder exercised reasonable care in safeguarding the Card from risk of loss or theft and, upon becoming aware of such loss or theft, promptly reported the loss or theft to the Program Manager.

# Visa Announces Designation Process for Consumer Reloadable Prepaid Cards

As announced in the 5 June 2014 edition of the Visa Business News, Visa has introduced a new designation for U.S. financial institutions and their agents (program managers and processors) that issue consumer reloadable prepaid cards.

## Consumer Reloadable Prepaid Standard

The Visa standard builds in flexibility to allow both for programs in which day-to-day activities are covered under an issuer-established monthly fee; and for programs that, in place of a single monthly fee, charge consumers only when they use their card for purchases, up to an issuer-established maximum monthly total fee.

To qualify for the Visa Prepaid designation, prepaid programs must meet the Visa Consumer Reloadable Prepaid Standard, which includes:

- Providing a transparent, simplified fee structure that covers day-to-day card use. Whether a program charges a single monthly fee (including purchase transactions) or, for less frequent card users, a fee only when the cardholder uses the card for purchases (up to an issuer-set monthly total), the following day-to-day activities must be offered at no charge to cardholders:
  - o Transaction declines
  - o Customer service
  - o In-network ATM withdrawals or balance inquiries<sup>2</sup>
  - o Cash back at the point of sale
  - o Card closures
- Providing transparent communications to cardholders about activities that are covered, whether under the issuer-set monthly fee or the maximum monthly total
- Not allowing for overdraft coverage or fees
- Permitting inactivity fees only if an account has been inactive for a certain period of time. Inactivity fees cannot exceed the maximum monthly fee, and the monthly fee cannot be charged in the same month.

**If you have any questions on the above articles please contact your client relationship manager.**

## GreenDot Network Updates

We would like to make you aware of a new Walgreens policy for prepaid cardholders. Effective immediately, Walgreens has chosen to institute a new policy where all General Purpose Reloadable (GPR) purchases (including swipe and MoneyPak® reloads) will prompt the associate to enter the customer's ID info. Any cardholder attempting to load more than \$500 in a 24-hour period will be declined.

While no other retailer has instituted this new policy, Walgreens is doing so in order to aggregate GPR sales across the chain, and ensure AML compliance. This policy was scheduled to roll out chain-wide by mid-August. It is important for you to alert your cardholders and customer care teams to the change in cardholder experience, especially cardholders that have reloaded at Walgreens previously without having to show ID.

**Below are answers to a few common questions:**

### What information will the POS capture?

ID Type, #, and State. POS will then prompt cashier to confirm or correct the data: Name, Address, DOB, and ID expiration date.

### When is this rolling out?

Rollout is scheduled to begin immediately, with full chain deployed by mid-August

### What forms of ID is Walgreens accepting?

US Driver's License  
State-issued ID  
Military ID  
Passport

### Questions

Please contact your Relationship Manager.

# Freeze Schedule 2014 – 2015

Please find below the current freeze schedule dates received to date by the bank from our processors and participating networks a final schedule will be sent to all program managers early November 2014.

Network/Processor Freeze Schedule			
<i>Processor</i>	<i>Start/End Date_Time</i>	<i>Impacts</i>	<i>Program Implementation Impacted</i>
<b>Fiserv</b>	Nov 24, 2014 - Dec 1, 2014	Changes to our system, operational processes, and network environment are limited during this time frame.including routine application and system program updates (for example, code changes) and normal implementation project activity (for example, ATM or parameter changes) will not be performed.  Applications include, but are not limited to, Card Management, Settlement Manager, Data Navigator, and your switch applicationChange requests submitted to EFT Product Support are not considered application system changes and will be allowed until Thursday, Dec. 11, 2014Change requests must be submitted to EFT Product Support no later than Wednesday, Dec. 3, 2014.	Yes
<b>FIS North</b>	Dec 14, 2014- Jan 3, 2015  Nov. 1, 2014 - Jan. 9, 2015		Possible
	Dec. 12, 2014 - Jan. 9, 2015	No Changes Year End Freeze	Yes
<b>i2c</b>	Dec 10, 2014 - TBD	Year End Freeze	Possible
<b>Store Financial</b>	Nov 15, 2014 - Jan 31, 2015	Development releases. BIN install can still happen as long as it doesn't fall in VISA's or MC's freeze dates.	Yes
<b>FiCentive</b>	Nov 26, 2014 - Dec 1, 2014	End-of-Year Freeze Schedule - Thanksgiving, Developmental Release	Possible
	Dec 22, 2014 - Jan 3, 2015	End-of-Year Freeze Schedule - Holiday, Developmental Release	Possible
<i>Networks</i>	<i>Start Date/Time</i>	<i>Impacts</i>	<i>Program Implementation Impacted</i>
<b>Visa</b>	Oct 17, 2014 - Oct 20, 2014	<b>October 2014 VisaNet Business Enhancements Release</b> During these control periods clients and processors should adjust their processing parameters and operational procedures accordingly. Clients are also encouraged to refrain from implementing or converting card programs during these periods as Visa will have limited ability to provide emergency system updates	Yes
	Nov 10, 2014 - Jan 3, 2014	<b>2014 Peak Season</b> During these control periods clients and processors should adjust their processing parameters and operational procedures accordingly. Clients are also encouraged to refrain from implementing or converting card programs during these periods as Visa will have limited ability to provide emergency system updates	
<b>MasterCard</b>	Oct 11, 2014 - Oct 22, 2014	Dual Message System (Authorization) and Single Message System Implementation/Dual Message System (Clearing) No customer-requested parameter changes may take effect on these business processing dates.	No
	Nov 3, 2014 - Nov 5, 2014	MIP Global Roll—Dual Message System (Authorization and Clearing) and Single Message System Implementation No customer-requested parameter changes can become effective on these business processing dates.	No
<b>NYCE</b>	Nov 26, 2014 ALL DAY	NYCE Network cannot be added into production on these dates	Yes
	December 17, 2014 ALL DAY	NYCE Network cannot be added into production on these dates	Yes
	December 24, 2014 ALL DAY	NYCE Network cannot be added into production on these dates	Yes
	December 31, 2014 ALL DAY	NYCE Network cannot be added into production on these dates	Yes
<b>STAR</b>	Ded 2, 2014 - Dec 18, 2014	The freeze parameters include all application and infrastructure changes in addition to participant, processor and ATM specification changes processed through Client Implementations, ATM Implementations and Processor Relations.	Yes
	Jan 5, 2015- Jan 18, 2015		Yes
<b>Pulse</b>	Nov 24, 2014 - Jan 3, 2015	Pulse Network cannot be added into production on these dates	Yes
<b>Accel/Exchange</b>		Changes to our system, operational processes, and network environment are limited during this time frame.including routine application and system program updates (for example, code changes) and normal implementation project activity (for example, ATM or parameter changes) will not be performed.	Yes
	Dec 14, 2014 - Jan 3, 2015		

# Prepaid Team Employee Spotlight



My name is **Dana Wehde**, and I have been with Sunrise Banks since February 2013 as the Prepaid Internal Auditor. Initially when I joined Sunrise, I worked on audits of Prepaid Policy and Prepaid operations in addition to performing annual and 90 day compliance reviews for our Prepaid Program Managers. In 2014 my role changed to concentrate more on the general Bank audits including audits for our National Products Division. Prior to coming to Sunrise Banks, I spent the last 5 years in the prepaid card industry at Meta Payment Systems as an Analyst and Internal Auditor. I also worked at Wells Fargo for six years, Educational Financial Service in various roles.

Personally, I have been married for 12 years and we have an eight year old son. Our lives are busy with sport activities from football, baseball and basketball. In my spare time, I enjoy playing recreation volleyball, reading and putting together puzzles.



My name is **Lacey Pressler**. I have been with Sunrise Banks since November 2012 as the Prepaid Billing and Implementation Specialist, working under Heather Schumacher implementing new processors and program managers, along with completing the monthly invoices and billing breakdown from our multiple networks. Prior to coming to Sunrise Banks, I spent 6 years in the prepaid card industry at Meta Payment Systems within a similar role.

Personally, I am married with two children, a 6 year old daughter and a 14 month old boy, along with the two kids we have a 2 year old Morkie named Lucy and an 8 year old Beagle named Harley. In our spare time my family enjoys watching movies, spending time with friends and family, boating and bike riding.