SOLIMAR
SYSTEMS

OPERATE WITH LESS SECURITY FRICTION:

Eliminate Customer Data Leaks Without Limiting Operations

Controls to prevent data leakage and unauthorized access are critical for every printer working with Personally Identifiable Information (PII) and other sensitive data. While protecting customer data in transactional and direct marketing environments is paramount, print providers must also balance operational needs that require sharing documents with other internal departments and external partners for customer support, technical troubleshooting, and daily business requirements.

Solimar Systems' redaction and obfuscation features are easy to implement and embed into automated workflow processes, so it becomes a standard option in your operations. Using these techniques to remove, obscure, or transform data so that it protects PII helps streamline business operations and minimizes issues with current and upcoming security legislation and audits. These technologies are an integral part of a multi-pronged data security and access strategy that should also include Zero-Trust Testing Environments.

Obfuscation

Obfuscation is a software rendering technique to obscure or make content unreadable by the human eye. It is useful to still view relative positioning of the content within the overall design. Solimar offers AFP-based obfuscation in Solimar® Print Director™ Enterprise (SPDE). Obfuscation is most commonly used in PDF files with ReadyPDF® Prepress Server.

Redaction

Redaction is object-level removal or hiding of specific design elements, such as the numbers of a credit card. Solimar offers sophisticated redaction capabilities using SOLindexer™ and Rubika®.

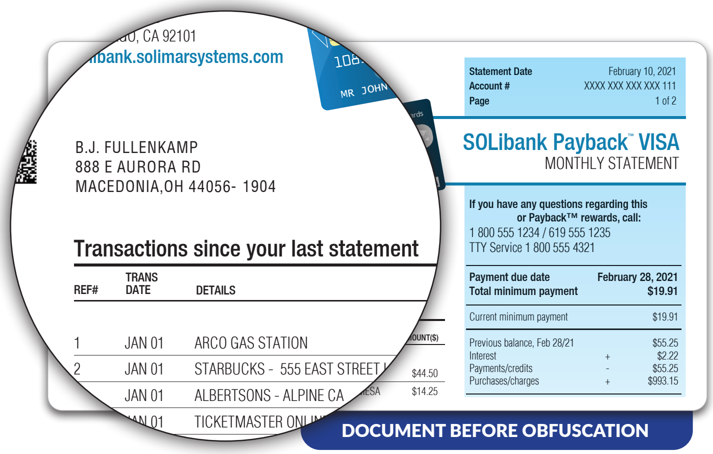
Prepared by: McGrew Group

Scan the barcode to request to receive ***Build a Zero-Trust Testing Environment with Solimar*** or other Solimar whitepapers.

What is Obfuscation?

Obfuscation, per the Oxford dictionary, is making something obscure, unclear or unintelligible. In the context of printed communications containing sensitive information, it means making the information unreadable and unintelligible for the recipient. Intended recipients can use the documents for business purposes, while unintended recipients, like those from data breaches, do not gain any leverageable information.

Solimar obfuscation features work on several levels to create an optimized and PII-secure document. Settings control what elements of the PDF document should be discarded. Users can control items that typically add bloat to the file structure without any benefit to the recipient, like attachments, JavaScript actions, and hidden content layers. Images and paths can also be discarded, if necessary. Next, options are set for how numbers and certain words are whitelisted to remain unchanged after the obfuscation process. Whitelisting these elements allows the recipient to understand the document structure, such as page numbers or section headings, but not any PII elements.



GO, CA 92101
ibank.solimarsystems.com

B.J. FULLENKAMP
888 E AURORA RD
MACEDONIA,OH 44056- 1904

Transactions since your last statement

REF#	TRANS DATE	DETAILS	OUNT($)
1	JAN 01	ARCO GAS STATION	
2	JAN 01	STARBUCKS - 555 EAST STREET L	$44.50
	JAN 01	ALBERTSONS - ALPINE CA ESA	$14.25
	AN 01	TICKETMASTER ONLIN	

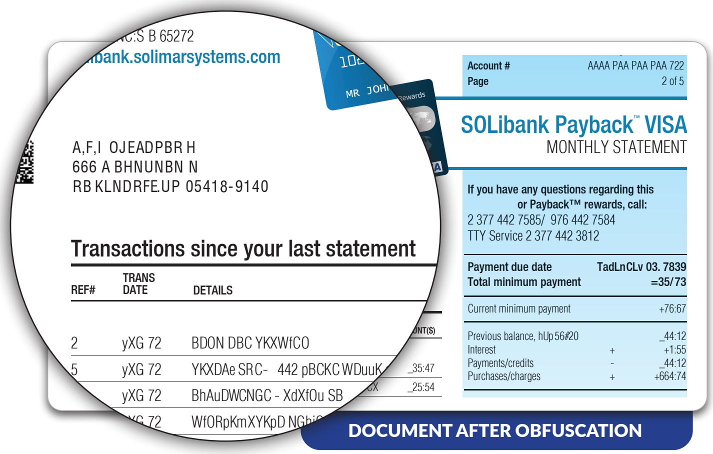
Statement Date	February 10, 2021
Account #	XXXX XXX XXX XXX 111
Page	1 of 2

SOLibank Payback™ VISA
MONTHLY STATEMENT

If you have any questions regarding this or Payback™ rewards, call:
1 800 555 1234 / 619 555 1235
TTY Service 1 800 555 4321

Payment due date		February 28, 2021
Total minimum payment		$19.91
Current minimum payment		$19.91
Previous balance, Feb 28/21		$55.25
Interest	+	$2.22
Payments/credits	-	$55.25
Purchases/charges	+	$993.15

DOCUMENT BEFORE OBFUSCATION



NC:S B 65272
ibank.solimarsystems.com

A,F,I OJEADPBR H
666 A BHNUNBN N
RB KLNDRFE.UP 05418-9140

Transactions since your last statement

REF#	TRANS DATE	DETAILS	UNT($)
2	yXG 72	BDON DBC YKXWfCO	
5	yXG 72	YKXDAe SRC- 442 pBCKC WDuuK	_35:47
	yXG 72	BhAuDWCNGC - XdXfOu SB CX	_25:54
	XG 72	WfORpKmXYKpD NGhi	

Account #	AAAA PAA PAA PAA 722
Page	2 of 5

SOLibank Payback™ VISA
MONTHLY STATEMENT

If you have any questions regarding this or Payback™ rewards, call:
2 377 442 7585/ 976 442 7584
TTY Service 2 377 442 3812

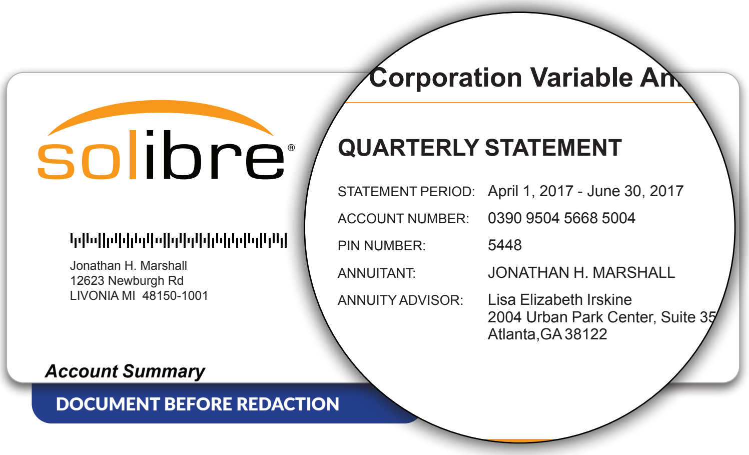
Payment due date		TadLnCLv 03. 7839
Total minimum payment		=35/73
Current minimum payment		+76:67
Previous balance, hUp 56#20		_44:12
Interest	+	+1:55
Payments/credits	-	_44:12
Purchases/charges	+	+664:74

DOCUMENT AFTER OBFUSCATION

What is Redaction?

Redaction edits text to hide or remove confidential or sensitive information. With Solimar redaction tools, the file is first indexed to understand and identify the relevant document structure and elements. Decisions and rules for specific elements can be created with Solimar tools to define how those items should be redacted or modified.

There are many ways to redact information. The text can be replaced randomly, with specific characters, or covered with an opaque rectangle, like using a permanent marker on a printed document. For advanced needs, regular expressions can be created as rules to find and modify specific characters based on a pattern match within the file.



solibre®

Jonathan H. Marshall
12623 Newburgh Rd
LIVONIA MI 48150-1001

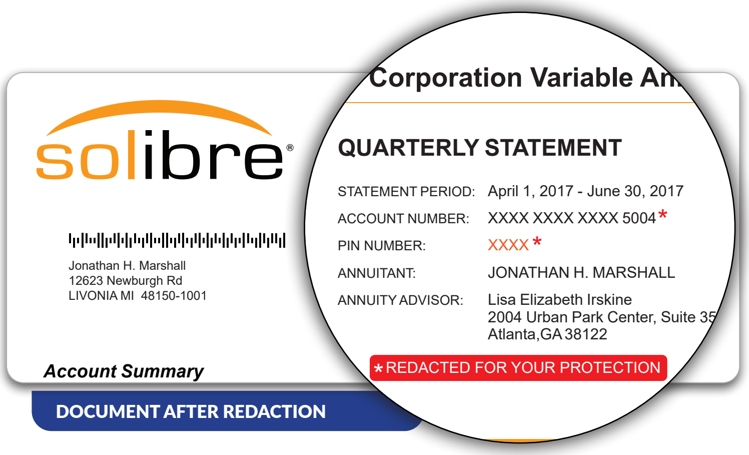
Account Summary

Corporation Variable An

QUARTERLY STATEMENT

STATEMENT PERIOD:	April 1, 2017 - June 30, 2017
ACCOUNT NUMBER:	0390 9504 5668 5004
PIN NUMBER:	5448
ANNUITANT:	JONATHAN H. MARSHALL
ANNUITY ADVISOR:	Lisa Elizabeth Irskine 2004 Urban Park Center, Suite 35 Atlanta,GA 38122

DOCUMENT BEFORE REDACTION



solibre®

Jonathan H. Marshall
12623 Newburgh Rd
LIVONIA MI 48150-1001

Account Summary

Corporation Variable An

QUARTERLY STATEMENT

STATEMENT PERIOD:	April 1, 2017 - June 30, 2017
ACCOUNT NUMBER:	XXXX XXXX XXXX 5004 *
PIN NUMBER:	XXXX *
ANNUITANT:	JONATHAN H. MARSHALL
ANNUITY ADVISOR:	Lisa Elizabeth Irskine 2004 Urban Park Center, Suite 35 Atlanta,GA 38122

* REDACTED FOR YOUR PROTECTION

DOCUMENT AFTER REDACTION

Obfuscation & Redaction Use Cases

Obfuscation and redaction fulfill the requirement to limit information beyond the primary owner of the PII. Below are six use cases where files must be shared or used for business operations while restricting access to sensitive customer data:

1

SHARING WITHIN THE PRINT SERVICE PROVIDER

Supporting customers is a cross-departmental effort. Customer support representatives need access to customer files to respond to inquiries. Creative and document composition teams need to confirm the design and positioning of elements after the data merge. Most internal staff should only be able to access PII-restricted files to ensure operations run smoothly, so redaction and obfuscation can be a standard, automated practice.

2

SHARING WITHIN THE CUSTOMER OPERATIONS

Similarly, customers may need to use documents throughout their organization to support their clients. Marketing and compliance teams, for example, need to validate any document redesign before implementing regulatory changes. These tools are essential because many stakeholders are involved in testing and validation when adding personalized offers to transaction documents.

3

SHARING WITH THIRD-PARTY VENDORS

Print service providers increasingly outsource custom development and programming based on talent or cost decisions. In some cases, development teams are handed datasets with minimum and maximum testing values, but in others, it helps to use a live data set. Obfuscating or redacting PII is a safe, best practice for sharing files to expedite development while minimizing risk.

Obfuscation & Redaction Use Cases *(continued)*

4

DIGITAL DELIVERY AND E-PRESENTMENT

Consumers want the flexibility of accessing their transactional statements and notifications on their own terms, whether in print, digital, or both. Digital channels present higher risks for interception and misuse, which can be mitigated by removing PII.

5

PROOFING AND APPROVAL BY THE CLIENT

The accuracy of customer data is as important as the security and use of that data. When there are client-facing dashboards for proofing and approval, these files and documents should be modified to restrict PII, like account numbers and address information.

6

MANAGING DATA ARCHIVES

With archiving and e-presentment services, the amount of data stored and managed is continuously increasing. There may also be customer-provided data hiding in IT, customer support, document composition, and other departments initially used to assist the customer but never discarded. Data at rest presents additional security risks, but they can be minimized if a redaction or obfuscation process is embedded into your overall workflow.

Redaction and obfuscation techniques aim to reduce the friction to your operations that security protocols and procedures dictate. Creating PII-restricted data whenever possible minimizes the security and operational risks to your operation, your customers, and their clients without burdening your existing workflows or staff. It is the smart move to make for your data-driven business.

Ready to discuss your needs and questions? Let's have a chat!
Ping us at SOLichat@solimarsystems.com

tel: +1.619.849.2800 • **www.solimarsystems.com**

© 2023. Solimar Systems, Inc. All rights reserved. Trademarks are property of their respective owners. REV 0723-v1.2