Compromised Identity Exchange: How to Contribute Compromised Data

The first step in protecting your customers from fraud following a data breach at your organization is to contribute your breached records to the Compromised Identity Exchange. In order to offer consumers the highest level of protection, XOR has outlined in this document the proper process and format to contribute this data to the exchange.

XOR implements the highest level of security and encryption standards at every stage of development and implementation to ensure that the Compromised Identity Exchange does not create additional risk of breach or opportunities for fraudsters to access exchange data.

Data received by XOR that does not meet the standards outlined here or that we feel creates consumer or business risk will not be accepted into the exchange, and will be deleted immediately.

Additionally, XOR follows stringent data minimization principles, and information is deleted following its use in the exchange. This prevents your customers' information from being used by any entity for marketing or other unintended purposes.

If you feel your organization is not prepared to follow these procedures for contributing breached data, contact info@xor.exchange for assistance.

Participation for compromised entities is free of charge and presents invaluable opportunity to protect your customers and limit the effects of your organization's data breach.

We welcome your participation and commitment to protecting consumers.

Implementation Process for Compromised Entities

There are two options for compromised entities to share breach information through the exchange:

1. Provide XOR with the personally identifiable information (PII) of the breached consumers as well as other basic information about the compromise event.

2. Install and run XOR's distributed exchange software that allows breached data to be matched in real time without any PII leaving your systems.

The remainder of this document focuses on the first option as it is the simplest and quickest way for a compromised entity to protect customers. If you would prefer not to send compromised PII outside of your organization, then please contact XOR for more information about how to install and run the distributed exchange software. XOR does not recommend this method unless your compromise involves more than 10,000 consumers.

Below is a description of the steps required to directly provide XOR with breach data. A detailed description of each step is provided below.

1. Signup for a secure data transfer account with XOR
2. Prepare compromised PII for transfer to XOR
3. Transfer compromised data to XOR
4. Submit compromise metadata to XOR

Signup for a Data Transfer Account

XOR hosts an SFTP server which can be used to securely transfer breached data to XOR. To get started, go to https://xor.exchange/breached and fill out the signup form. Once the form has been submitted, we will provide you with the necessary information to be able to login to the system.

XOR will not accept file transfers over insecure channels such as email. In the event that data is sent to XOR in such a manner, the data will be immediately deleted.

Prepare Compromised PII for transfer to XOR

In keeping with XOR's data minimization standards, consumer information is deconstructed to the maximum extent possible prior to matching in the Compromised Identity Exchange. This is accomplished using a process developed by XOR called ID Factoring, which involves deconstructing identities into prime factors which are not individually sensitive but can be meaningfully matched. The most sensitive part of consumer's identity is not any particular element such as the SSN or name, but the combination of these elements.

Appendix A provides a detailed layout of the various ID Factored files that can be sent to XOR. It is not necessary to provide each of the different ID factors if, for example, you do not have emails or SSNs for all the affected

consumers; however, the more data that is provided the better the match will be. Appendix B provides the required layout if ID Factoring is not run.

To make this process easier, XOR will provide a free program to manage this process that will run on a wide variety of systems. Compromised entities are also free to implement their own processes as long as the files ultimately sent to XOR match the specifications. If your organization is unable to complete the ID Factoring process, contact XOR and we will determine the best format for you to send your data.

Transfer Compromised Data to XOR

Once the compromised data has been prepared to these specifications, you can transfer the data to XOR using your data transfer account. Once your data has been received, XOR will send you a confirmation email providing you with a unique ID for your breach. This is the ID that you will use to provide XOR with further information about your breach. In the event that there is more than one compromise event, information about each breach should be submitted separately and you will receive separate IDs for each occurrence.

Despite the fact that the transmission of data is already encrypted, XOR also prefers that all breached data sent to XOR be encrypted at a file level. This can be accomplished by using XOR's public PGP key which will be provided along with the account login information for your file transfer account.

Submit Compromised Metadata to XOR

After you have received your confirmation email from XOR you will need to provide information about the compromise event. This includes details such as the date the breach was detected and how the data was exposed (e.g., lost laptop, external hack, etc.). This information must be submitted to XOR before the data can be properly used by at-risk entities.

In the email confirming receipt of your data, XOR will provide a link to a Web form which must be completed prior to your data being activated in the exchange. This information will be gathered at the individual compromise level, so in the event that you have experienced multiple compromises you will need to fill out the form one time for each compromise event.

Once this form has been submitted, XOR will make your data available as part of the exchange. If you are interested in receiving additional reporting about how your data is being accessed and used to protect exposed consumers, please contact XOR.

Appendix A: ID Factored File Layouts

All files should be Unicode encoded and pipe ("|") delimited. All files should contain a header and each field listed below should always exist for each file. If a field is optional and will not be provided, please fill with two quotation marks ("").

Name and DOB Factor Layout

Field Name	Optional/Required	Formatting
Name ID	R	A unique string for each record. Should not match between files
First Name	R	All capital letters
Last Name	R	All capital letters
Middle Initial	O	A single capital letter
Name Suffix	O	All capital letters
Date of Birth	R	YYYY-MM-DD

SSN Factor Layout

Field Name	Optional/Required	Formatting
SSN ID	R	A unique string for each record. Should not match between files
SSN	R	9 digits (no dashes)

Address Factor Layout

Field Name	Optional/Required	Formatting
Address ID	R	A unique string for each record. Should not match between files

Address Line 1	R	Numbers followed by capital letters or P.O. Box
Address Line 2	O	"Unit" followed by a number
City	O	All capital letters
State	O	Two letter postal abbreviation
Zip Code	R	5 or 9 digits (no dashes)

Phone Request

Field Name	Optional/Required	Formatting
Phone ID	R	A unique string for each record. Should not match between files
Phone Number	R	10 digits (no dashes or parenthesis)

Email Request

Field Name	Optional/Required	Formatting
Email ID	R	A unique string for each record. Should not match between files
Email	R	user@domain

Appendix B: Non-ID Factored Layout

All files should be Unicode encoded and pipe ("|") delimited. All files should contain a header and each field listed below should always exist for each file. If a field is optional and will not be provided, please fill with two quotation marks ("").

Field Name	Optional/Required	Formatting
Record ID	R	A unique string for each record.
First Name	R	All capital letters
Last Name	R	All capital letters
Middle Initial	O	A single capital letter
Name Suffix	O	All capital letters
Date of Birth	R	YYYY-MM-DD
SSN	R	9 digits (no dashes)
Address Line 1	R	Numbers followed by capital letters or P.O. Box
Address Line 2	O	"Unit" followed by a number
City	O	All capital letters
State	O	Two letter postal abbreviation
Zip Code	R	5 or 9 digits (no dashes)
Phone Number	R	10 digits (no dashes or parenthesis)
Email	R	user@domain