



**OXFORD UNIVERSITY BANK**  
 Return Mail Processing Center  
 P.O. Box 6336  
 Portland, OR 97228-6336

<<Mail ID>>  
 <<Name 1>>  
 <<Name 2>>  
 <<Address 1>>  
 <<Address 2>>  
 <<Address 3>>  
 <<Address 4>>  
 <<Address 5>>  
 <<City>><<State>><<Zip>>  
 <<Country>>

<<Date>>

**Re: Notice of Data Breach**

Dear <<Name 1>>:

Oxford University Bank was recently notified by one of its vendors, American Bank Systems, or ABS, about a data security incident at ABS that may have affected your personal information. Although ABS has informed us that it has no evidence of identity theft or fraud as a result of this incident, this letter provides details of the incident, our response, and resources available to you to help protect your personal information from possible misuse, should you feel it is appropriate to do so.

**What Happened?** On October 22, 2020, ABS became aware that it was victimized by a cybercriminal and certain systems were infected with malware, which resulted in disruptions to certain ABS operations. ABS took its systems offline and launched an investigation into the nature and scope of the incident. With the assistance of third-party computer forensic specialists, ABS has determined that certain documents stored within ABS’s environment were subject to unauthorized access or acquisition. On October 27, 2020, their investigation determined that information related to Oxford University Bank customers was part of the information affected, and ABS provided a list of potentially affected customers to the bank on November 6, 2020.

**What Information Was Involved?** The investigation by ABS determined your name and the following types of data were present in the documents that were identified as accessed or taken by the unauthorized actor: <<Data Elements>>. At this time, we are unaware of any identity theft or fraud as a result of this incident.

**What We Are Doing.** Upon discovering this incident, ABS took steps to assess the security of its systems and mitigate the impact of this incident, including by resetting passwords. ABS also reviewed existing security policies and implemented additional measures, including advanced endpoint monitoring, to further protect information in their care. Oxford University Bank also assessed the security of its internal systems and determined that no internal bank systems were compromised.

Although we are unaware of any identity theft or fraud as a result of this incident, ABS is offering you access to <<CM Length>> months of credit monitoring and identity theft protection services through TransUnion at no cost to you as an added precaution. If you wish to activate these services, you may follow the instructions included in the attached *Steps You Can Take to Protect Your Information*. We encourage you to enroll in these services as we are unable to act on your behalf to do so.

**What You Can Do.** You should remain vigilant against incidents of identity theft and fraud, and you should review your account statements and monitor your credit reports for suspicious activity and to detect errors for the next 12 to 24 months. If you suspect fraud in your accounts, please report such activity. Please also review the information contained in the attached *Steps You Can Take to Protect Your Information*.

**For More Information.** We understand that you may have questions about this incident that are not addressed in this letter. If so, please contact our toll-free dedicated assistance line at 855-914-4705 between 8:00 am and 8:00 pm Central Standard Time, Monday through Friday. You may also call us directly at (662) 234-6668.

Oxford University Bank strives daily to earn our customers' trust and ensure that they know their customer information is protected. We are in this together and will provide customer support as needed.

Sincerely,

A handwritten signature in black ink, appearing to read "David Guyton", with a long horizontal flourish extending to the right.

David Guyton  
President and CEO

## STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

### **Enroll in Credit Monitoring**

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for <<CM Length>> months provided by TransUnion Interactive, a subsidiary of TransUnion,<sup>®</sup> one of the three nationwide credit reporting companies.

### **How to Enroll: You can sign up online or via U.S. mail delivery**

- To enroll in this service, go to the *myTrueIdentity* website at [www.MyTrueIdentity.com](http://www.MyTrueIdentity.com) and, in the space referenced as “Enter Activation Code,” enter the 12-letter Activation Code <<Insert Unique 12-letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode <<Insert static 6-digit Telephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

### **ADDITIONAL DETAILS REGARDING YOUR COMPLIMENTARY CREDIT MONITORING SERVICE:**

- Once you are enrolled, you will be able to obtain <<CM Length>> months of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

### **Monitor Accounts**

Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. We recommend periodically obtaining credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus listed below directly to request a free copy of your credit report.

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

<b>Experian</b> P.O. Box 9554 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com/freeze/center.html">www.experian.com/freeze/center.html</a>	<b>TransUnion</b> P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 <a href="http://www.transunion.com/credit-freeze">www.transunion.com/credit-freeze</a>	<b>Equifax</b> P.O. Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 <a href="http://www.equifax.com/personal/credit-report-services">www.equifax.com/personal/credit-report-services</a>
---	--	---

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;

4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

<p><b>Experian</b>  P.O. Box 9554  Allen, TX 75013  1-888-397-3742  <a href="http://www.experian.com/fraud/center.html">www.experian.com/fraud/center.html</a></p>	<p><b>TransUnion</b>  P.O. Box 2000  Chester, PA 19016  1-888-680-7289  <a href="http://www.transunion.com/fraud-victim-resource/place-fraud-alert">www.transunion.com/fraud-victim-resource/place-fraud-alert</a></p>	<p><b>Equifax</b>  P.O. Box 105069  Atlanta, GA 30348  1-888-766-0008  <a href="http://www.equifax.com/personal/credit-report-services">www.equifax.com/personal/credit-report-services</a></p>
--	--	---

You can further educate yourself regarding identity theft prevention, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

**For District of Columbia residents**, the Attorney General for the District of Columbia may be contacted at 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; (202) 727-3400; and <https://oag.dc.gov>.

**For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662; 1-888-743-0023; or [www.oag.state.md.us](http://www.oag.state.md.us).

**For New Mexico residents**, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf), or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

**For New York residents**, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

**For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000; or [www.ncdoj.gov](http://www.ncdoj.gov). You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

**For Rhode Island Residents**, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, Rhode Island 02903; [www.riag.ri.gov](http://www.riag.ri.gov); or 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are approximately 3 Rhode Island residents whose information may have been impacted by this incident.

# Oxford University Bank Incident Log

**Reported by**

- **Name:** David Guyton
- **Phone:** 662-234-6668
- **Email:** davidguyton@oubol.com
- **Method of Contact:** by phone

**Date and time of incident detection:**

ABS – Became aware of an issue on October 23, 2020 and confirmed the issue on October 29, 2020.

Bank – Became aware on November 3, 2020 and assembled the Incident Response Team.

**Nature of Incident:**

- **Denial of Service**
- **Malicious Code (worm, virus)**
- **Scans and Probes**
- **Unauthorized access**
- **Website Defacement**
- **Other (describe):** Malware

**Incident description and severity (what were the signs?):**

ABS's President/CEO, Jay Bruce, contacted David Guyton by phone to inform him that ABS had become aware of an incident in which data, including customers' sensitive information, had been fraudulently removed from ABS's environment. The Bank was never aware of this event until the phone call to David.

**System affected: (include device name, location, IP address at the time of attack, and MAC address)**

BankManager - software OUB uses which sets up new loan/deposit customer files, links those customers with related customer files, tracks collateral, and files the documents in e-folders specifically designed for banks.

**Details: (virus name, events, data loss, etc.)**

On October 23, 2020, OUB's third party service provider, American Bank Systems (ABS - BankManager), became aware that it was victimized by a cybercriminal and that certain systems were infected with malware, which resulted in disruptions to certain ABS operations. Certain data, including bank customers' information was removed from ABS's environment. ABS was in possession of customers' information due to an upcoming conversion. The information included the following - names, addresses, social security numbers (for some), dates of birth (for some), and account numbers for 12,881 individual customers; and names, addresses, and account numbers for 1,411 corporate/business customers.

**Business Impact: (what information or services are impacted, estimated monetary loss)**

At this point, there has been no monetary loss recognized. This has the potential to cause harm to the Bank's reputation.

**Course of Action: (include dates, times, and contact information for communications/notifications, blocking/unblocking, law enforcement/regulatory notifications, and recovery actions taken)**

Members of the Incident Response team (David Guyton, Audra Cook, Heather Humphreys, and Kimberly Buford) met on November 3, 2020 at 1:30 p.m. to sit in on a call with Jay Bruce, ABS President/CEO to discuss the details of the incident and to determine our next course of action. The plan was find out exactly what information was removed/compromised, but in the meantime, to get the Bank's legal counsel involved in the process.

**Incident Level:**

Level 1 (most critical) – Unauthorized disclosure, modification, destruction or deletion of sensitive information or data; disruption of business continuity and critical business processes and communication; incident impacting public perception

**Additional Notes:**

On 11/10/20, the removed/compromised information was received by the bank and forwarded to the bank's legal counsel for review. The bank's legal counsel is currently in the process of developing a letter appropriate in response to the situation to send to affected customers. In the meantime, the bank plans to assign personnel to field calls to answer questions and offer any help needed related to this incident.

## David Guyton

---

**From:** Jay Bruce <jbruce@abs-ok.com>  
**Sent:** Tuesday, November 03, 2020 5:27 PM  
**To:** David Guyton  
**Subject:** Confidential  
**Attachments:** ABS Notice Letter to Oxford University Bank.11-3-20.pdf

David,

Attached is our letter notifying you of the cyber-attack incident and the proposed letter that we would send to your customers on your behalf, but only with your approval. Again, we regret the incident has affected your Bank and customers. We are working diligently with the team of attorneys and computer forensic specialists to respond to the incident.

With best regards,

Jay

James W. Bruce  
President/CEO & General Counsel



14000 Parkway Commons Drive  
Oklahoma City, OK 73134  
405.607.7000  
[www.americanbanksystems.com](http://www.americanbanksystems.com)

CONFIDENTIALITY NOTICE: This email, including any attachments, contains information that may be confidential or privileged. The information is intended to be for the use of the individual or entity names above. If you are not the intended recipient, be aware that any disclosure, copying, distribution or use of the contents of this information is prohibited. If you have received this email in error, please notify the sender immediately by "reply to sender only" message and destroy electronic and hard copies of the communication, including attachments.



American Bank Systems, Inc.

James W Bruce, III  
President & CEO  
14000 Parkway Commons Drive  
Oklahoma City, Oklahoma 73134  
405 605 7329 tel  
jbruce@abs-ok.com

Mr. David Guyton, President  
Oxford University Bank  
1500 University Avenue  
Oxford, MS 38655

November 3, 2020

Dear David,

American Bank Systems (“ABS”) writes to notify Oxford University Bank (the “Bank”) of an incident that may affect the security of certain Bank information, including Bank customer information, provided to ABS as part of normal business operations. We are providing you with information about this incident and our response to date.

**What Happened?** On October 23, 2020, ABS became aware that it was victimized by a cybercriminal and certain systems were infected with malware, which resulted in disruptions to certain ABS operations. We immediately took systems offline and launched an investigation into the nature and scope of the incident. With the assistance of third-party computer forensic specialists, we are working to investigate the source of the disruption, confirm its impact on our systems, and restore full functionality to our systems as soon as possible. Our investigation determined that an unauthorized individual removed certain data from the ABS environment. On October 27, 2020, our ongoing investigation determined that information related to Bank customers was part of the information removed from the environment. At this time, we do not have any evidence that your bank’s information was specifically targeted or subject to misuse; however, we are providing you this notice in the event you determine that notice is required to your customers who may be impacted.

**What Information Was Involved?** ABS reviewed the affected information to determine what information was impacted. The investigation into this event is ongoing and the scope of impacted data may be updated; however, we did not want to delay making you aware of the event. We determined that the names, addresses, phone numbers, dates of birth (for some), Social Security numbers (for some), and financial account numbers of 12,881 individual customers were included in the impacted data. We also determined that names, addresses, and financial account numbers were impacted for 1,411 corporate/business customers. Please contact us by email at [jbruce@abs-ok.com](mailto:jbruce@abs-ok.com) or by phone at 405.605.7329 so we may provide you with this information by secure transmission.

**What We Are Doing?** Information privacy and security are among our highest priorities. Upon discovering this incident, we immediately took steps to assess the security of our systems and mitigate the impact of this incident, including by resetting passwords. We also reviewed existing

Mr. David Guyton  
November 3, 2020  
Page 2

security policies and implemented additional measures, including advanced endpoint monitoring, to further protect information in our care.

**What You Can Do.** Under applicable law, your company may be required to provide notice of this incident to the affected individuals, as well as certain regulators. We are unable to provide you with legal advice and recommend you discuss the contents of this letter and your company's potential notification duties with your own legal counsel should you require legal guidance. In the event you determine you have a notice obligation to the customers, we can do the following upon your request and approval:


- Mail notification letters to customers identified to explain the incident and our subsequent investigation. Attached as *Exhibit A* is a sample of the notice letter we will mail on your behalf if approved.
- For the individuals for whom you request notification assistance, we will provide these notice recipients with access to 12 months of credit monitoring and identity theft protection services.
- Provide a toll-free telephone number to respond to customers' questions about this incident.

In order for us to take action to complete notifications on your behalf, please direct us to do so by November 16, 2020 by email to [jbruce@abs-ok.com](mailto:jbruce@abs-ok.com). Please list your company's name in the subject of the email. **We will not take any action described above on your behalf without your authorization.** If you determine that you have an obligation under applicable law to notify federal or state regulators as well as individuals, we will complete such notification only upon your specific additional direction.

**For More Information.** If you have questions about this incident, you may contact me by phone at 405.605.7329, via email to [jbruce@abs-ok.com](mailto:jbruce@abs-ok.com), or by writing to us at 14000 Parkway Commons Drive, Oklahoma City, Oklahoma 73134.

We sincerely regret this incident. You are a valued Customer. Protecting your information is important to us, and we are taking steps to enhance and strengthen measures to safeguard the information in our care.

Sincerely,



James W. Bruce, III  
President & CEO

Attachment





Mr. David Guyton  
November 3, 2020  
Page 3

Exhibit A

[ABS Letterhead/Logo]  
[First Name] [Last Name]  
[Address]  
[City, State, Zip Code]

[Date]

**Re: Notice of Data Breach**

Dear [First Name] [Last Name]:

American Bank Systems (“ABS”) provides electronic loan administration software to its bank partners, including [BANK], and writes to notify you of an incident that may affect the privacy of some of your personal information. ABS takes the protection of your information very seriously, and although we have no evidence of identity theft or fraud as a result of this incident, this letter provides details of the incident, our response, and resources available to you to help protect your personal information from possible misuse, should you feel it is appropriate to do so.

**What Happened?** On October 23, 2020, ABS became aware that it was victimized by a cybercriminal and certain systems were infected with malware, which resulted in disruptions to certain ABS operations. We immediately took systems offline and launched an investigation into the nature and scope of the incident. With the assistance of third-party computer forensic specialists, we are working to investigate the source of the disruption, confirm its impact on our systems, and restore full functionality to our systems as soon as possible. The investigation determined that certain documents stored within ABS’s environment were subject to unauthorized access or acquisition. On October 27, 2020, our investigation determined that information related to [Data Owner/Bank Name] customers was part of the information affected. ABS provided notice of the incident to [Data Owner/Bank Name] on [date] and worked to determine address information to provide notice of the incident. On [date], we completed this review.

**What Information Was Involved?** Our investigation determined your name and the following types of data were present in the documents that were identified as accessed or taken by the unauthorized actor: [DATA ELEMENTS]. At this time, we are unaware of any identity theft or fraud as a result of this incident.

**What We Are Doing.** Information privacy and security are among our highest priorities. Upon discovering this incident, we immediately took steps to assess the security of our systems and mitigate the impact of this incident, including by resetting passwords. We also reviewed existing security policies and implemented additional measures, including advanced endpoint monitoring, to further protect information in our care.



Mr. David Guyton  
November 3, 2020  
Page 4

Although we are unaware of any identity theft or fraud as a result of this incident, we are offering you access to [X] months of credit monitoring and identity theft protection services through [vendor] at no cost to you as an added precaution. If you wish to activate these services, you may follow the instructions included in the attached *Steps You Can Take to Protect Your Information*. We encourage you to enroll in these services as we are unable to act on your behalf to do so.

**What You Can Do.** We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity and to detect errors for the next 12 to 24 months. If you suspect fraud in your accounts, please report such activity to [Data Owner/Bank Name]. Please also review the information contained in the attached *Steps You Can Take to Protect Your Information*.

**For More Information.** We understand that you may have questions about this incident that are not addressed in this letter. If so, please contact our toll-free dedicated assistance line at [Call center number] between X:00 am and X:00 pm [time zone], Monday through Friday. You may also write to ABS at 14000 Parkway Commons Drive, Oklahoma City, Oklahoma 73134.

Sincerely,

[signatory]  
American Bank Systems



## STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

### Enroll in Credit Monitoring

[Insert credit monitoring language]

### Monitor Accounts

Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. We recommend periodically obtaining credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus listed below directly to request a free copy of your credit report.

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

#### **Experian**

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742

[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

#### **TransUnion**

P.O. Box 160  
Woodlyn, PA 19094  
1-888-909-8872

[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

#### **Equifax**

P.O. Box 105788  
Atlanta, GA 30348-5788  
1-800-685-1111

[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;

