

COVINGTON

BEIJING BOSTON BRUSSELS DUBAI FRANKFURT
JOHANNESBURG LONDON LOS ANGELES NEW YORK
PALO ALTO SAN FRANCISCO SEOUL SHANGHAI WASHINGTON

Covington & Burling LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001-4956
T +1 202 662 6000

Via Electronic Mail

October 2, 2024

Maryland Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Update to Notice of Security Incident Pursuant to Md. Code Ann., Com. Law § 14-3501 *et seq.*

To Whom it May Concern:

In accordance with the above-referenced provision of Maryland law, I write on behalf of Exeter Finance LLC ("Exeter") to provide an update regarding a security incident involving third party Financial Business and Consumer Solutions ("FBCS"). FBCS initially notified you of this incident on April 29, 2024.

As described in the April 29, 2024 notification and subsequent updates, in connection with providing debt collection services for Exeter-owned accounts, FBCS had been granted access to certain information from Exeter, including information about Exeter accounts. On April 5, 2024, Exeter received notification from FBCS that an information security incident on FBCS's systems involved information about Exeter accounts. Exeter understands that on or about February 26, 2024, FBCS discovered unauthorized access to certain systems on its network that occurred between February 14, 2024 and February 26, 2024. The information involved may have included a combination of an individual's name, address, Social Security number, date of birth, driver's license number, and/or financial account number. FBCS also indicated to Exeter that in response to the incident, it implemented additional safeguards in a newly built environment.

FBCS provided notice to the potentially affected residents of Maryland on Exeter's behalf between April 26, 2024 and May 17, 2024. Exeter also instructed FBCS to provide notice to the regulators in jurisdictions where individuals involved resided in accordance with applicable law in each jurisdiction, including Maryland. As noted above, FBCS initially notified you of this incident on April 29, 2024, and subsequently included Exeter among the data owners on whose behalf this notice was provided.

On July 18, 2024, FBCS informed Exeter through counsel that its data review determined that consumer information related to additional affected Exeter individuals could have been accessed and/or exfiltrated during the above-referenced incident. The information involved included the

COVINGTON

Maryland Office of the Attorney General
October 2, 2024
Page 2

same potential data elements referenced above. Upon receiving this update from FBCS, Exeter conducted its own review of the information involved and determined that information regarding approximately 547 additional Maryland residents (for a total of approximately 909 Maryland residents) affiliated with Exeter accounts was potentially affected.

After concluding its review of the additional information, Exeter moved as expediently as possible to notify the individuals involved and regulators. Attached to this email is a copy of the individual notice letter Exeter sent on August 16, 2024 to the 547 additional Maryland residents whose information was involved. Exeter has also provided 12 months of complimentary credit monitoring and identity restoration services to these individuals.

Though FBCS previously stated to Exeter that it would provide updates to regulators regarding this incident on Exeter's behalf, Exeter recently learned that FBCS has filed a petition for bankruptcy and is no longer in a position to do so. Exeter is therefore updating you directly in the interest of providing this information in a prompt manner.

If you have any questions or need further information regarding this incident, please feel free to contact me.

Respectfully submitted,

/s/ Caleb Skeath

Caleb W. Skeath
Counsel to Exeter Finance
LLC

Enclosure



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>>

Notice of Data << Event/Breach>>

Dear <<Name 1>>:

Exeter Finance LLC (“Exeter”) is writing to notify you of an incident at a third party, Financial Business and Consumer Solutions, Inc. (“FBCS”), that affects the privacy of some of your information. This letter provides details of the incident and the resources available to you to help protect your information should you feel it is appropriate to do so.

What Happened? FBCS, the third party that experienced this incident, provided debt collection services for certain Exeter-owned accounts. In connection with these services, FBCS received information about the individuals associated with these accounts. Exeter understands from FBCS that on February 26, 2024, FBCS discovered unauthorized access to certain systems in its network. This incident did not impact Exeter’s computer systems. FBCS informed Exeter that it took steps to secure the impacted environment and launched an investigation with the assistance of third-party computer forensics specialists to determine the nature and scope of the incident.

According to FBCS, the investigation determined that its environment was subject to unauthorized access between February 14 and February 26, 2024, and the unauthorized actor had the ability to view or acquire certain information on the FBCS network during the period of access. Exeter understands that FBCS undertook a review of the data at risk to assess if any sensitive information could be affected and to whom it related. We are notifying you because we have learned from FBCS that certain information related to you may have been accessed or exfiltrated during the incident. This notification was not delayed as a result of a law enforcement investigation.

What Information Was Involved? The types of information potentially affected by this incident include your: <<Data Elements>>. According to FBCS, there is no indication that your information has been misused in relation to this event.

What We Are Doing. Upon discovering this incident, we understand that FBCS immediately took steps to conduct an investigation to determine the nature and scope of the incident and also implemented additional safeguards in a newly built environment.

As an added precaution, we are offering you access to complimentary credit monitoring and identity restoration services for <<12/24>> months through CyEx. Please review the attached *Steps You Can Take to Help Protect Your Personal Information* for instructions regarding how to enroll and for additional information regarding these services. Please note you will need to enroll yourself in these services if you wish to do so, as we are not able to activate the services on your behalf.

What You Can Do. You can review the enclosed *Steps You Can Take to Help Protect Your Personal Information*. In addition, we encourage you to remain vigilant against incidents of identity theft and fraud, to monitor your account statements to detect errors, and to review your credit reports for suspicious activity. We also encourage you to enroll in the complimentary credit monitoring services we are offering you.

For More Information. We understand you may have questions about the incident that are not addressed in this letter. If you have questions, please call 877-851-5249 between 9:00 AM and 9:00 PM ET Monday through Friday excluding major U.S. holidays. Additionally, you can write to FBCS at 330 S. Warminster Road, Suite 353, Hatboro, PA 19040.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

Enroll in Credit Monitoring



Identity Defense

<<Name 1>>
Enter your Activation Code: <<Activation Code>>
Enrollment Deadline: <<Enrollment Deadline>>
Service Term: <<12/24>> Months*

Identity Defense Complete

Key Features

- 1-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- \$1 Million Identity Theft Insurance**

Enrollment Instructions

To enroll in Identity Defense, visit **app identitydefense.com/enrollment/activate/exe**

1. **Enter your unique Activation Code <<Activation Code>>**
Enter your Activation Code and click 'Redeem Code'.
2. **Create Your Account**
Enter your email address, create your password, and click 'Create Account'.
3. **Register**
Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
4. **Complete Activation**
Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is <<Enrollment Deadline>>. After <<Enrollment Deadline>>, the enrollment process will close, and your Identity Defense code will no longer be active. If you do not enroll by <<Enrollment Deadline>>, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at 1.866.622.9303.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit 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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you may need to provide the following information, depending on whether you make the request online, by phone, or by mail:

*Service Term begins on the date of enrollment, provided that the enrollment takes place during the approved enrollment period.

**Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert P.O. Box 9554 Allen, TX 75013	TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; 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, your state Attorney General, and the Federal Trade Commission.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and <https://oag.dc.gov>.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting https://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 New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>. The Department of State Division of Consumer Protection can be contacted at: Department of State, Albany Location, One Commerce Plaza, 99 Washington Ave, Albany, NY 12231-0001; 1-800-697-1220; or <http://dos.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and <https://www.ncdoj.gov>.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; <https://www.riag.ri.gov>; and 1-401-274-4400. Under Rhode Island law, individuals have the right to file or obtain any police report filed in regard to this event. There are approximately <<#>> Rhode Island residents that may be impacted by this event.



Fox Rothschild LLP
Two Commerce Square
2001 Market Street
Suite 1700
Philadelphia, PA 19103
Tel 215.299.2000 Fax 215.299.2150
www.foxrothschild.com

Michael G. Menkowitz

Direct Dial: (215) 299-2756
Internet Address: mmenkowitz@foxrothschild.com

November 27, 2024

Office of the Maryland Attorney General
200 Saint Paul Place
Baltimore, MD 21202

Re: Supplemental Notice of Data Security Incident

To Whom It May Concern:

We represent Christine C. Shubert, Chapter 7 Trustee for the estate of Financial Business and Consumer Solutions ("FBCS"). As you may know, FBCS filed a voluntary petition for relief under chapter 7 of title 11 of the United States Code on August 29, 2024, which is pending in the United States Bankruptcy Court for the Eastern District of Pennsylvania, Case No. 24-1329.

We understand that FBCS previously notified your office of a data security incident that impacted residents in your state. The Trustee has been requested by a former customer of FBCS to notify you that 1,067 additional letters were mailed to Maryland residents between September 18-23, 2024. We understand this is in addition to letters previously sent by FBCS. The Trustee was not provided a copy of those letters, and she does not have any further information about the original notification or the above subsequent notification. We have located a publicly available sample notification letter previously reported by FBCS to the California Attorney General, a copy of which is attached as Exhibit A. We also suspect that the letter used in the subsequent notification was substantially the same as the sample letter previously provided to your office.

A Pennsylvania Limited Liability Partnership

If you have any questions, please contact me at (215) 299-2756 or mmenkowitz@foxrothschild.com.

Very truly yours,

A handwritten signature in blue ink, appearing to be 'MG' with a stylized flourish.

Michael G. Menkowitz
For Fox Rothschild LLP

Exhibit A

(attached hereto)



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

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

<<Date>>

Notice of Data << Event/Breach>>

Dear <<Name 1>>:

Financial Business and Consumer Solutions, Inc. ("FBCS") is writing to notify you of an incident that may affect the privacy of some of your information. FBCS is a debt collection agency, and this letter provides details of the incident and the resources available to you to help protect your information should you feel it is appropriate to do so.

What Happened? On February 26, 2024, FBCS discovered unauthorized access to certain systems in its network. This incident did not impact computer systems outside of FBCS's network. We immediately took steps to secure the impacted environment and launched an investigation with the assistance of third-party computer forensics specialists to determine the full nature and scope of the incident. The investigation determined that the environment was subject to unauthorized access between February 14 and February 26, 2024, and the unauthorized actor had the ability to view or acquire certain information on the FBCS network during the period of access. Therefore, FBCS undertook a comprehensive review of the data at risk to assess if any sensitive information could be affected and to whom it related. We are notifying you because certain information related to you may have been accessed or exfiltrated during the incident. This notification was not delayed as a result of a law enforcement investigation.

What Information Was Involved? The types of information potentially affected by this incident include your: <<Data Elements>>. FBCS has no indication that your information has been misused in relation to this event.

What We Are Doing. Upon discovering this incident, we immediately took steps to conduct a diligent investigation to confirm the nature and scope of the incident. As part of FBCS's ongoing commitment to the security of information on our platform, we also implemented additional safeguards in a newly built environment.

As an added precaution, we are offering you access to complimentary credit monitoring and identity restoration services for <<12/24>> months through CyEx. Please review the attached *Steps You Can Take to Help Protect Your Personal Information* for instructions regarding how to enroll and for additional information regarding these services. Please note you will need to enroll yourself in these services if you wish to do so, as we are not able to activate the services on your behalf.

What You Can Do. You can review the enclosed *Steps You Can Take to Help Protect Your Personal Information*. In addition, we encourage you to remain vigilant against incidents of identity theft and fraud, to monitor your account statements to detect errors, and to review your credit reports for suspicious activity. We also encourage you to enroll in the complimentary credit monitoring services we are offering you.

For More Information. We understand you may have questions about the incident that are not addressed in this letter. If you have questions, please call 888-984-6614 between 9:00 AM and 9:00 PM ET Monday through Friday excluding major U.S. holidays. Additionally, you can write to us at 330 S. Warminster Road, Suite 353, Hatboro, PA 19040.

Sincerely,

Amy Stratz
Executive Vice President
Financial Business and Consumer Solutions, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

Enroll in Credit Monitoring



<<Name 1>>

Enter your Activation Code: <<Activation Code>>

Enrollment Deadline: <<Enrollment Deadline>>

Service Term: <<12/24>> Months*

Identity Defense Complete

Key Features

- 1-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- \$1 Million Identity Theft Insurance**

Enrollment Instructions

To enroll in Identity Defense, visit app.identitydefense.com/enrollment/activate/fbcs

1. Enter your unique Activation Code <<Activation Code>>

Enter your Activation Code and click 'Redeem Code'.

2. Create Your Account

Enter your email address, create your password, and click 'Create Account'.

3. Register

Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.

4. Complete Activation

Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is <<Enrollment Deadline>>. After <<Enrollment Deadline>>, the enrollment process will close, and your Identity Defense code will no longer be active. If you do not enroll by <<Enrollment Deadline>>, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at 1.866.622.9303.

*Service Term begins on the date of enrollment, provided that the enrollment takes place during the approved enrollment period.

**Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit 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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you may need to provide the following information, depending on whether you make the request online, by phone, or by mail:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert P.O. Box 9554 Allen, TX 75013	TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; 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, your state Attorney General, and the Federal Trade Commission. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and <https://oag.dc.gov>.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting https://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 New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and <https://www.ncdoj.gov>.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; <https://www.riag.ri.gov>; and 1-401-274-4400. Under Rhode Island law, individuals have the right to file or obtain any police report filed in regard to this event. There is/are approximately <<RI Count>> Rhode Island residents that may be impacted by this event.



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

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

<<Date>>

Notice of Data << Event/Breach>>

Dear <<Name 1>>:

Financial Business and Consumer Solutions, Inc. (“FBCS”) is a debt collection agency, providing services to <<Data Owner>>. FBCS is writing on behalf of <<Data Owner>> to notify you of an incident that affects the privacy of some of your information. This letter provides details of the incident and the resources available to you to help protect your information should you feel it is appropriate to do so.

What Happened? On February 26, 2024, FBCS discovered unauthorized access to certain systems in its network. This incident did not impact computer systems outside of FBCS’s network, including any systems belonging to <<Data Owner>>. We immediately took steps to secure the impacted environment and launched an investigation with the assistance of third-party computer forensics specialists to determine the full nature and scope of the incident. The investigation determined that the environment was subject to unauthorized access between February 14 and February 26, 2024, and the unauthorized actor had the ability to view or acquire certain information on the FBCS network during the period of access. Therefore, FBCS undertook a comprehensive review of the data at risk to assess if any sensitive information could be affected and to whom it related. We are notifying you because certain information related to you may have been accessed or exfiltrated during the incident. This notification was not delayed as a result of a law enforcement investigation.

What Information Was Involved? The types of information potentially affected by this incident include your: <<Data Elements>>. FBCS has no indication that your information has been misused in relation to this event.

What We Are Doing. Upon discovering this incident, we immediately took steps to conduct a diligent investigation to confirm the nature and scope of the incident. As part of FBCS’s ongoing commitment to the security of information on our platform, we also implemented additional safeguards in a newly built environment. As an added precaution, we are offering you access to complimentary credit monitoring and identity restoration services for <<12/24>> months through CyEx. Please review the attached *Steps You Can Take to Help Protect Your Personal Information* for instructions regarding how to enroll and for additional information regarding these services. Please note you will need to enroll yourself in these services if you wish to do so, as we are not able to activate the services on your behalf.

What You Can Do. You can review the enclosed *Steps You Can Take to Help Protect Your Personal Information*. In addition, we encourage you to remain vigilant against incidents of identity theft and fraud, to monitor your account statements to detect errors, and to review your credit reports for suspicious activity. We also encourage you to enroll in the complimentary credit monitoring services we are offering you.

For More Information. We understand you may have questions about the incident that are not addressed in this letter. If you have questions, please call 888-984-6614 between 9:00 AM and 9:00 PM ET Monday through Friday excluding major U.S. holidays. Additionally, you can write to us at 330 S. Warminster Road, Suite 353, Hatboro, PA 19040.

Sincerely,

Amy Stratz
Executive Vice President
Financial Business and Consumer Solutions, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

Enroll in Credit Monitoring



<<Name 1>>

Enter your Activation Code: <<Activation Code>>

Enrollment Deadline: <<Enrollment Deadline>>

Service Term: <<12/24>> Months*

Identity Defense Complete

Key Features

- 1-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- \$1 Million Identity Theft Insurance**

Enrollment Instructions

To enroll in Identity Defense, visit app.identitydefense.com/enrollment/activate/fbcs

1. Enter your unique Activation Code <<Activation Code>>

Enter your Activation Code and click 'Redeem Code'.

2. Create Your Account

Enter your email address, create your password, and click 'Create Account'.

3. Register

Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.

4. Complete Activation

Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is <<Enrollment Deadline>>. After <<Enrollment Deadline>>, the enrollment process will close, and your Identity Defense code will no longer be active. If you do not enroll by <<Enrollment Deadline>>, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at 1.866.622.9303.

*Service Term begins on the date of enrollment, provided that the enrollment takes place during the approved enrollment period.

**Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit 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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you may need to provide the following information, depending on whether you make the request online, by phone, or by mail:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert P.O. Box 9554 Allen, TX 75013	TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; 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, your state Attorney General, and the Federal Trade Commission. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and <https://oag.dc.gov>.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting https://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 New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and <https://www.ncdoj.gov>.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; <https://www.riag.ri.gov>; and 1-401-274-4400. Under Rhode Island law, individuals have the right to file or obtain any police report filed in regard to this event. There is/are approximately <<RI Count>> Rhode Island residents that may be impacted by this event.