P.O. Box 30285
Salt Lake City, UT 84130-0285

November 6, 2024

By Email
Office of the Attorney General
1125 Washington St. SE, PO Box 40100
Olympia, WA 98504
SecurityBreach@atg.wa.gov

To Whom It May Concern:

This letter provides an update to a notice your office first received on April 26, 2024 regarding a cybersecurity incident that occurred at Financial Business and Consumer Solutions, Inc. ("FBCS"), a debt collection agency engaged by Kohl's to perform services in connection with the Kohl's credit card. At that time Capital One, as issuer of the Kohl's credit card, had determined to notify impacted individuals of the incident along with appropriate state authorities, pending additional investigation by FBCS into the incident. On behalf of Capital One, FBCS provided initial notice to your office.

FBCS has now completed its investigation and has identified additional impacted individuals associated with the provision of services for Kohl's card customers. We are providing notice directly to you because after having made initial notifications on our behalf, FBCS declared bankruptcy. Capital One has reviewed the results of FBCS' investigation and determined that a total of 7,735 Washington individuals for which Capital One is a data owner—rather than the 3,167 Washington individuals previously identified—have been confirmed to have been impacted by the FBCS incident. Notification letters were mailed to individuals who were not previously notified. Such letters were sent on or about August 15, 2024. This notice is to ensure compliance with Wash Rev. Code Ann. § 19.255.010 given FBCS' recent filing of bankruptcy.

Should you have any questions, please contact me at the information below.

Respectfully yours,

Adam Cohen, Senior Director, Associate General Counsel Cyber Legal
Capital One Financial Corp
1680 Capital One Drive
McLean, VA 22102-3491
(571) 308-5971
DSE_Contact@capitalone.com

PIERSON FERDINAND

MICHAEL E. KAR
PARTNER

Rockefeller Center
1270 Avenue of the Americas
7th Floor
New York, NY 10020

Direct: 1.631.215.3415
Email: michael.kar@pierferd.com

November 13, 2024

Via Email (securitybreach@atg.wa.gov)

Washington State Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

Re: Third-Party Data Incident
Financial Business and Consumer Solutions, Inc. – February 26, 2024

To Whom It May Concern:

Pierson Ferdinand LLP represents First Financial Portfolio Venture Capital, LLC and First Financial Investment Fund Holdings, LLC ("FFP"), located at 3091 Governors Lake Drive, Suite 500, Peachtree Corners, Georgia 30071, and its related entities, including: First Financial Investment Fund III, LLC, First Financial Investment Fund V, LLC, First Financial Investment Fund VI, LLC, First Portfolio Ventures I, LLC and First Portfolio Ventures II, LLC.

This correspondence is related to the data breach notification previously made to your office by Financial Business and Consumer Solutions, Inc. ("FBCS") arising out of a February 26, 2024 incident (the "FBCS Incident"). See attached ***Enclosure A*** notification made by FBCS, which includes notice on behalf of FFP. FFP is a third-party impacted by the FBCS Incident.

We understand that FBCS mailed incident notification letters to certain impacted data subjects before completing data mining. FBCS subsequently advised that additional impacted individuals were identified, informed FFP that FBCS would not mail any further data subject notification letters, and declared bankruptcy. FFP is now providing notification to additionally impacted individuals identified by FBCS. We note that FBCS provided public data breach notice via webpage and notice to media outlets.

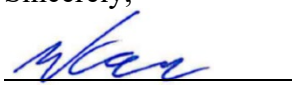
FBCS has not reported instances of data misuse or fraud.

FFP contacted impacted third-party entities regarding the additional impacted data subjects. On October 17, 2024, FFP mailed breach notification letters to the data subjects identified by FBCS that were not otherwise sent notifications. This notification was based on the notification previously made by FBCS, and a template is enclosed as ***Enclosure B***. Letters were mailed to

1,266 residents of your state. FFP is also providing complimentary credit monitoring, identity theft protection, and call center services.

FFP values the protection and proper use of personal information and will continue to mitigate harm while hardening its third-party cyber risk. If you have any questions or need additional information, please do not hesitate to contact me at michael.kar@pierferd.com or +1(631) 215-3415.

Sincerely,



Michael E. Kar
Partner
Pierson Ferdinand LLP

Enclosures (2)

Enclosure A

From: William Judge
Sent: Wednesday, May 29, 2024 5:57 PM
To: Brooke, Donnelle M (ATG) <donnelle.brooke@atg.wa.gov>
Cc: Christopher DiIenno <cdiienno@mullen.law>; Lora Funston <lfunston@mullen.law>; Katharin DiRosa <kdirosa@mullen.law>; Maxwell Beermann <mbeermann@mullen.law>; Lynn Montgomery <lmontgomery@mullen.law>; Maxwell Beermann <mbeermann@mullen.law>
Subject: RE: Summary of 05/23/24 Call Re New Notices for FBCS Data Owners

Dear Donnelle,

Thank you for the update on the below.

We continue to work with the involved data owners and develop letters with the requested information broken out for each data owner. In the meantime, as we continue to data-mine and notify impacted individuals, we wanted to update you on additional entities and impact to WA residents. These new entities and individuals will be incorporated into the detailed letters to be sent in response to your request.

Best,
Bill

William Judge
Attorney
Mullen Coughlin LLC
426 W. Lancaster Avenue, Suite 200
Devon, PA 19333
(267) 930-6813 - Office
(610) 613-2837 - Mobile
wjudge@mullen.law

From: Brooke, Donnelle M (ATG) <donnelle.brooke@atg.wa.gov>
Sent: Tuesday, May 28, 2024 3:25 PM
To: Christopher DiIenno <cdiienno@mullen.law>; William Judge <wjudge@mullen.law>
Subject: Summary of 05/23/24 Call Re New Notices for FBCS Data Owners

Dear Mr. DiIenno and Mr. Judge,

Thank you so much for speaking with me last Thursday regarding the process needed for the Financial Business and Consumer Solutions, Inc. notices. As mentioned in our call, we need individual notices for each data owner which was impacted by the FBCS security incident. I believe the easiest solution would be for me to manually create a notice in our WebForm for each data owner. The information which was originally uploaded on 04/26/24 for Financial Business and Consumer Solutions is what I will use for each notice that I create. The only difference will be the name change and the amount of WA residents. The 04/26/24 notification date to our office will be used as well.

I will need a cover letter from you with the name of each data owner and the total amount of WA residents impacted. I only need ones for those who had more than 500 WA residents. Right now, I show the following:

American First Finance, LLC – 1,799
Capital One (as issuer of a Kohl's credit card) - 3,148
Elan Financial Services – 1,371
US Bank – 4,965
Vivint, Inc. – 559

I do not need a letter for Truist Bank (260) or Regional Acceptance (81) unless the numbers have changed. In the event you do get more residents and need to notify us, we can use the same 04/26/24 as the notification date as well since you did technically notify me already for these two.

Please feel free to email the letters for each to securitybreach@atg.wa.gov. You can send all letters in one email if that is easier. I oversee that email box so they will come directly to me. In addition, if you have supplemental information for

any of the data owners mentioned, can you provide the information in letter format, as a PDF attachment, to a separate email for each. (Hopefully that made sense). You can send them to the same email address.

I think that is everything. If I left anything out or if would like to speak with me at any point, please do not hesitate to reach out.

Thank you again,

Donnelle

Donnelle Brooke
Paralegal | Consumer Protection Division
WA State Office of the Attorney General
800 Fifth Avenue, Suite 2000
Seattle, WA 98104
Phone-206-464-6562
Donnelle.Brooke@atg.wa.gov

Christopher J. DiIenno
Office: (267) 930-4775
Fax: (267) 930-4771
Email: cdilenno@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

May 29, 2024

VIA E-MAIL

Washington State Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
E-mail: securitybreach@atg.wa.gov

Re: Supplemental Notice of Data Event

To Whom It May Concern:

As you may know, we represent Financial Business and Consumer Solutions, Inc. ("FBCS") located at 330 South Warminster Road, Suite 353, Hatboro, Pennsylvania 19040. We write to supplement our April 26, 2024, notice to your office (the "April 26 Notice") and our May 10, 2024 supplemental notice to your office (the "May 10 Notice"). By providing this supplemental notice, FBCS does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Notice to Washington Residents

Since the submission of this notice, FBCS has continued its efforts to identify and notify additional affected individuals. On May 29, 2024, FBCS mailed notice to an additional four thousand three hundred seventy-three (4,373) Washington residents. As such, thirty-six thousand five hundred fifty-three (36,553) total potentially impacted Washington residents have been provided with notice. The information that could have been subject to unauthorized access includes name, Social Security number, date of birth, account information and medical information. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A.***

Other Steps Taken and To Be Taken

In addition to the steps taken, which were more fully discussed in the April 26 Notice, FBCS is providing access to credit monitoring services for twelve (12) months, through Cyex, to individuals

whose personal information was potentially affected by this incident, at no cost to these individuals.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4775.

Very truly yours,

Christopher J. DiIenno of
MULLEN COUGHLIN LLC

CJD/lcf
Enclosure

EXHIBIT A

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

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/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

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/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.

Archived: Thursday, May 30, 2024 5:28:48 PM
From: William Judge
Sent: Thu, 30 May 2024 14:38:51
To: Katharin DiRosa
Subject: FW: Summary of 05/23/24 Call Re New Notices for FBCS Data Owners
Importance: Normal
Sensitivity: None
Attachments:
Financial Business and Consumer Solutions - Notice of Data Event - WA.pdf; Financial Business and Consumer Solutions - Regulator Notice Addendum - WA.pdf;

William Judge
Attorney
Mullen Coughlin LLC
426 W. Lancaster Avenue, Suite 200
Devon, PA 19333
(267) 930-6813 - Office
(610) 613-2837 - Mobile
wjudge@mullen.law

From: William Judge
Sent: Wednesday, May 29, 2024 5:57 PM
To: Brooke, Donnelle M (ATG) <donnelle.brooke@atg.wa.gov>
Cc: Christopher DiIenno <cdiienno@mullen.law>; Lora Funston <lfunston@mullen.law>; Katharin DiRosa <kdirosa@mullen.law>; Maxwell Beermann <mbeermann@mullen.law>; Lynn Montgomery <lmontgomery@mullen.law>; Maxwell Beermann <mbeermann@mullen.law>
Subject: RE: Summary of 05/23/24 Call Re New Notices for FBCS Data Owners

Dear Donnelle,

Thank you for the update on the below.

We continue to work with the involved data owners and develop letters with the requested information broken out for each data owner. In the meantime, as we continue to data-mine and notify impacted individuals, we wanted to update you on additional entities and impact to WA residents. These new entities and individuals will be incorporated into the detailed letters to be sent in response to your request.

Best,
Bill

William Judge
Attorney
Mullen Coughlin LLC
426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

(267) 930-6813 - Office
(610) 613-2837 - Mobile
wjudge@mullen.law

From: Brooke, Donnelle M (ATG) <donnelle.brooke@atg.wa.gov>
Sent: Tuesday, May 28, 2024 3:25 PM
To: Christopher DiIenno <cdiienno@mullen.law>; William Judge <wjudge@mullen.law>
Subject: Summary of 05/23/24 Call Re New Notices for FBCS Data Owners

Dear Mr. DiIenno and Mr. Judge,

Thank you so much for speaking with me last Thursday regarding the process needed for the Financial Business and Consumer Solutions, Inc. notices. As mentioned in our call, we need individual notices for each data owner which was impacted by the FBCS security incident. I believe the easiest solution would be for me to manually create a notice in our WebForm for each data owner. The information which was originally uploaded on 04/26/24 for Financial Business and Consumer Solutions is what I will use for each notice that I create. The only difference will be the name change and the amount of WA residents. The 04/26/24 notification date to our office will be used as well.

I will need a cover letter from you with the name of each data owner and the total amount of WA residents impacted. I only need ones for those who had more than 500 WA residents. Right now, I show the following:

American First Finance, LLC – 1,799
Capital One (as issuer of a Kohl's credit card) - 3,148
Elan Financial Services – 1,371
US Bank – 4,965
Vivint, Inc. – 559

I do not need a letter for Truist Bank (260) or Regional Acceptance (81) unless the numbers have changed. In the event you do get more residents and need to notify us, we can use the same 04/26/24 as the notification date as well since you did technically notify me already for these two.

Please feel free to email the letters for each to securitybreach@atg.wa.gov. You can send all letters in one email if that is easier. I oversee that email box so they will come directly to me. In addition, if you have supplemental information for any of the data owners mentioned, can you provide the information in letter format, as a PDF attachment, to a separate email for each. (Hopefully that made sense). You can send them to the same email address.

I think that is everything. If I left anything out or if would like to speak with me at any point, please do not hesitate to reach out.

Thank you again,

Donnelle

Donnelle Brooke
Paralegal | Consumer Protection Division
WA State Office of the Attorney General
800 Fifth Avenue, Suite 2000
Seattle, WA 98104
Phone-206-464-6562
Donnelle.Brooke@atg.wa.gov

Christopher J. DiIenno
Office: (267) 930-4775
Fax: (267) 930-4771
Email: cdiienno@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

May 28, 2024

VIA E-MAIL

Washington State Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
E-mail: securitybreach@atg.wa.gov

Re: Initial List of Data Owners

To Whom It May Concern:

Below, please find an initial list of data owners on whose behalf Financial Business and Consumer Solutions, Inc. ("FBCS") has reported this matter to your office:

First Portfolio Ventures I, LLC
First Portfolio Ventures II, LLC
First Financial Investment Fund III, LLC

Please let us know if you have any questions.

Very truly yours,

Christopher J. DiIenno of
MULLEN COUGHLIN LLC

CJD/lcf

Data Breach Notification Form

Thank you for your submission. An automatic email will be sent to cdiienno@mullen.law with a copy of the materials you submitted.

Data Breach Notification Form

The form was not submitted. Please correct the problems below and resubmit the form.

- **Required: Notice Washington Residents**

IMPORTANT: Please do not use this form to provide updates to a previously submitted notice. Please send all updates to SecurityBreach@atg.wa.gov (mailto:SecurityBreach@atg.wa.gov), and include the date of submission of the original notice you provided. Thank you.

*** Required Information**

1 Entity Details

***Name of Entity**

(The name of the company/agency/entity that experienced data-breach)

Financial Business and Consumer Solutions, Inc.

Url Address

Washington State Unified Business ID

Number of employees

118

*** Address**	*** City**	**State**	***Zip**
330 South Warminster R	Hatboro	PA	19040

***Phone**

(215) 320-3033

***Industry Affected**

Business

***Business Sub-Category:**	***If Other, explain:**
Other	Professional Services

2 Breach Detail

***When did the entity first become aware an incident took place**

2/26/2024

***Start of Breach**		***End of Breach**	
2/14/2024	☐ Unknown	2/26/2024	☐ Unknown

Start of Investigation

End of Investigation

3rd Party Forensic Firm/Security Firm

***Information Compromised**

- [x] Name
- [x] Social Security Number
- [x] Driver's License or Washington ID Card Number
- [x] Financial & Banking Information
- [x] Full Date of Birth
- [ ] Unique Private Key (e.g. used to authenticate or sign an electronic record)
- [ ] Student ID Number
- [ ] Military ID Number
- [ ] Passport Number
- [x] Health Insurance Policy or ID Number
- [x] Medical Information
- [ ] Biometric Data
- [ ] Username and Password/Security Question Answers
- [ ] Email Address and Password/Security Question Answers
- [ ] Other

***# of Washingtonians Affected**

25,175 ☐ Unknown

***Cause of Breach**

Cyberattack

***Cyberattack Type**

Ransomware

Other Breach Causes or Attacks

Please see Exhibit 1.

***Summary of Steps Taken to Contain the Breach**

Please see Exhibit 1.

3 Notice to Washington Residents

***Date notice provided**

4/26/2024

***Did the notice include the three credit agencies?**

Yes

***Form of Notice**

- ☐ Electronic
- ☑ Written
- ☐ Substitute

Upload Attachments You may upload **5 files** with a total file size limit of **20 megabytes**.
Please provide the following documents as well as any supporting documentation (PDF Only):

- **Cover Letter to Attorney General's Office**

  Choose File Financial Bu...t 1 - WA.pdf

- ***Notice to Washington Residents**

  Choose File Financial Bu...t 1 - WA.pdf

- **Other Attachments**

  Choose File No file chosen

4 Contact Information

***Last Name**

Dilenno

***First Name**

Christopher

Middle Name

***Organization/Law Firm Name**

Mullen Coughlin LLC

***Address**

426 W. Lancaster Ave, Si

***City**

Devon

***State**

PA

***Zip**

19333

***Phone**

(267) 930-4775

***E-Mail Address**

cdiienno@mullen.law

***Confirm E-Mail Address**

cdiienno@mullen.law

A confirmation email containing a copy of your completed submission will be emailed to the address provided.

5 Public Record Disclosure and Signature

***** I acknowledge that the information provided, including the attachments, once submitted will be posted on the Attorney General Office's public facing website and may constitute a public record.

☑ I understand

I declare, under penalty of perjury under the laws of the State of Washington, that the information contained in this complaint is true and accurate, and that any documents attached are true and accurate copies of the originals.

***Name**

Christopher Dilenno

***Declared this date**

4/26/2024

***City:**

Devon

***State:**

PA

I'm not a robot

reCAPTCHA
Privacy - Terms

Submit

EXHIBIT 1

The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, neither FBCS, nor its clients, waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

FBCS is a third-party debt collection agency and receives personal information from its clients, which is used to collect debts on behalf of its clients.

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 those of its clients. FBCS 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. FBCS undertook a comprehensive review of the data at risk to determine if any sensitive information could be affected and to whom it related. FBCS learned that certain information provided by customer organizations related to individuals may have been accessed or exfiltrated during the incident. FBCS has seen no evidence of misuse of any information related to this incident.

Starting on April 4, 2024, FBCS began providing notice of this incident to potentially impacted clients, and as the investigation and review of the data continued, reported to its clients what specific data of theirs was impacted. FBCS then offered to provide notice on behalf of its clients to potentially impacted individuals as required.

The information that could have been subject to unauthorized access includes name, Social Security number, date of birth, and account information.

Notice to Washington Residents

Beginning on April 26, 2024, FBCS began providing written notice of this incident to individuals, which includes twenty-five thousand one hundred seventy-five (25,175) Washington residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, FBCS moved quickly to investigate and respond to the incident, assess the security of FBCS systems, and identify potentially affected individuals. Further, FBCS notified federal law enforcement regarding the event. FBCS is also working to implement additional safeguards in a newly built environment. FBCS is providing access to credit monitoring services for twelve (12) months, through Cyex, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, FBCS is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. FBCS is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

FBCS is providing notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A

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

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/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

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/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.

Enclosure B

c/o Epiq
Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

Notice of Data << Incident/Breach>>

Dear <<Name 1>>:

Financial Business and Consumer Solutions, Inc. ("FBCS") is a debt collection agency that provides services to creditors and related organizations, including <<data owner>> ("FFP"). FBCS is a third-party that notified FFP of an incident that may affect the privacy of some of your information, and therefore FFP is notifying individuals identified by FBCS as potentially impacted by the incident. This letter provides details of the incident as reported by FBCS, along with the resources available to you to help protect your information should you feel it is appropriate to do so.

What Happened? As reported by FBCS, on February 26, 2024, FBCS discovered unauthorized access to certain systems in its network. FBCS 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, 2024 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. FBCS identified 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? FBCS has advised that the types of information potentially affected by this incident vary by individual, and could have included: <<Breached Elements>>. FBCS has no indication that your information has been misused in relation to this event.

What FBCS and FFP Are Doing. We understand that upon discovering this incident, FBCS 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 its platform, FBCS also implemented additional safeguards in a newly built environment. As an added precaution, FFP is offering 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. 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 that we are offering you.

For More Information. We understand you may have questions about the FBCS incident that are not addressed in this letter. FFP has reported and will provide any information received from FBCS regarding this FBCS incident. If you have questions, please call 877-438-1237 between 8:00 AM and 8:00 PM CT Monday through Friday excluding major U.S. holidays. Additionally, you can write to FBCS at 330 S. Warminster Road, Suite 353, Hatboro, PA 19040.

Sincerely,

<<data owner>>

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/ffam**

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 <<#>> Rhode Island residents that may be impacted by this event.>>

c/o Epiq
Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

Notice of Data << Incident/Breach>>

Dear <<Name 1>>:

Financial Business and Consumer Solutions, Inc. ("FBCS") is a debt collection agency that provides services to creditors and related organizations. This includes accounts previously and not currently owned by <<data owner>> ("FFP"). FBCS is a third-party that notified FFP of an incident that may affect the privacy of some of your information, and therefore FFP is notifying individuals identified by FBCS as potentially impacted by the incident. This letter provides details of the incident as reported by FBCS, along with the resources available to you to help protect your information should you feel it is appropriate to do so.

What Happened? As reported by FBCS, on February 26, 2024, FBCS discovered unauthorized access to certain systems in its network. FBCS 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, 2024 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. FBCS identified 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? FBCS has advised that the types of information potentially affected by this incident vary by individual, and could have included: <<Breached Elements>>. FBCS has no indication that your information has been misused in relation to this event.

What FBCS and FFP Are Doing. We understand that upon discovering this incident, FBCS 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 its platform, FBCS also implemented additional safeguards in a newly built environment. As an added precaution, FFP is offering 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. 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 that we are offering you.

For More Information. We understand you may have questions about the FBCS incident that are not addressed in this letter. FFP has reported and will provide any information received from FBCS regarding this FBCS incident. If you have questions, please call 877-438-1237 between 8:00 AM and 8:00 PM CT Monday through Friday excluding major U.S. holidays. Additionally, you can write to FBCS at 330 S. Warminster Road, Suite 353, Hatboro, PA 19040.

Sincerely,

<<data owner>>

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/ffam**

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 <<##>> Rhode Island residents that may be impacted by this event.>>

APPENDIX A

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

Dear <<Full Name>>:

We are writing to notify you of a data security incident involving some of your information that occurred at Financial Business and Consumer Solutions (FBCS), a third party service provider previously used by Comcast. Although FBCS experienced the security incident, we are taking initiative to support any former and present customers who have been impacted. This notice explains the incident, measures we have taken and some steps you can take in response.

What Happened? On March 13, 2024, FBCS notified Comcast that it had experienced a data breach incident, but that Comcast consumer data was not impacted. However, on July 17, 2024, FBCS notified Comcast of its new finding that Comcast data was impacted. FBCS provided the following information: "[f]rom February 14 and February 26, 2024, an unauthorized party gained access to FBCS's computer network and some of its computers. During this time, the unauthorized party downloaded data from FBCS systems and encrypted some systems as part of a ransomware attack. Upon discovering the attack on February 26, 204, FBCS launched an investigation with the assistance of third-party cybersecurity specialists. In the course of that investigation, FBCS discovered that the files downloaded by the unauthorized party contained personal information, including personal information about you. FBCS also notified the Federal Bureau of Investigation (FBI) of this attack."

This security incident occurred entirely at FBCS and not at Xfinity or on Comcast systems. FBCS notified Comcast that due to its current financial status, it would no longer able to provide notices or credit monitoring protection to individuals impacted by the incident. As such, we are contacting you directly and providing support services. FBCS received your information because they previously provided Comcast with collections-related services for delinquent payments until 2020, when Comcast ceased working with FBCS. The compromised information about you dates from around 2021, as FBCS is subject to data retention requirements beyond Comcast's working relationship with FBCS.

What Information Was Involved? FBCS's investigation discovered that files downloaded by the unauthorized party included your name, address, Social Security number, date of birth, and your Comcast account number and ID numbers used internally at FBCS. FBCS states that it has no indication that any personal information compromised during this incident has been further misused.

What We Are Doing. We are offering you complimentary identity theft protection services for at least 12 months through membership in CyEx Identity Defense Complete, which includes credit monitoring services. Since FBCS informed Comcast of this incident on July 17, 2024, Comcast has been working with FBCS to understand how the incident occurred and to notify affected individuals (including you) and appropriate governmental authorities. As stated above, Comcast no longer uses FBCS. Notifications about this incident have not been delayed due to law enforcement investigation.

What You Can Do. In addition to enrolling in the identify theft protection services referenced above at no cost to you, we encourage you (as we always encourage all our customers) to remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. Please review the "Additional Steps You Can Take" information enclosed with this letter. We also encourage all of our customers to better protect their Xfinity accounts by signing up for two-step verification.[1] All customers should remain alert for unusual or suspicious emails or telephone calls. Information about common scams and how to protect yourself and your Xfinity account are available on our website.[2]

For More Information. We sincerely regret any inconvenience caused by this incident. If you have any questions, please call 888-769-8426, Monday through Friday, between 9:00 am and 9:00 pm, Eastern Time, Monday through Friday.

Sincerely,

Comcast

[1] Learn more at https://www.xfinity.com/support/articles/two-step-verification-xfinity-app-setup
[2] https://www.xfinity.com/support/articles/protect-yourself-phone-scams

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

- **Additional Free Resources on Identity Theft**: You can obtain information from the consumer reporting agencies, the FTC (https://www.identitytheft.gov/) or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the Federal Trade Commission or to the Attorney General in your state. You may want to contact your state Attorney General to obtain further information. Below is the contact information for the Attorneys General for residents of New York, North Carolina, Rhode Island, Oregon, the District of Columbia, and Maryland.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

New York Attorney General
Office of the Attorney General
The Capitol
Albany, NY 12224-0341
https://ag.ny.gov/
1-800-771-7755

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
401-274-4400

Oregon Attorney General
100 SW Market Street
First Floor
Tilikum Room
Portland, OR 97201
https://www.doj.state.or.us/consumer-protection/
1-877-877-9392

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, D.C. 20001
oag@dc.gov
https://oag.dc.gov/

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
https://www.marylandattorneygeneral.gov/
Main number: 410-576-6300
Toll-free: 1-888-743-0023
Consumer Hotline: 410-528-8662

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses listed above.

You'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Comcast Corporation, 1701 John F. Kennedy Boulevard, Philadelphia, PA 19103, 888-769-8426.

Identity Defense

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

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 {{URL}}

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.

Christopher J. DiIenno
Office: (267) 930-4775
Fax: (267) 930-4771
Email: cdiienno@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

April 29, 2024

VIA E-MAIL

Washington State Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
E-mail: securitybreach@atg.wa.gov

Re: Initial List of Data Owners

To Whom It May Concern:

Below, please find an initial list of data owners on whose behalf Financial Business and Consumer Solutions, Inc. ("FBCS") has reported this matter to your office:

American First Finance, LLC
Capital One (as issuer of a Kohl's credit card)
Elan Financial Services
Truist Bank and Regional Acceptance
U.S. Bank
Vivint, Inc.

Please let us know if you have any questions.

Very truly yours,

Christopher J. DiIenno of
MULLEN COUGHLIN LLC

CJD/lcf
Enclosure

EXHIBIT 1

The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, neither FBCS, nor its clients, waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

FBCS is a third-party debt collection agency and receives personal information from its clients, which is used to collect debts on behalf of its clients.

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 those of its clients. FBCS 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. FBCS undertook a comprehensive review of the data at risk to determine if any sensitive information could be affected and to whom it related. FBCS learned that certain information provided by customer organizations related to individuals may have been accessed or exfiltrated during the incident. FBCS has seen no evidence of misuse of any information related to this incident.

Starting on April 4, 2024, FBCS began providing notice of this incident to potentially impacted clients, and as the investigation and review of the data continued, reported to its clients what specific data of theirs was impacted. FBCS then offered to provide notice on behalf of its clients to potentially impacted individuals as required.

The information that could have been subject to unauthorized access includes name, Social Security number, date of birth, and account information.

Notice to Washington Residents

Beginning on April 26, 2024, FBCS began providing written notice of this incident to individuals, which includes twenty-five thousand one hundred seventy-five (25,175) Washington residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, FBCS moved quickly to investigate and respond to the incident, assess the security of FBCS systems, and identify potentially affected individuals. Further, FBCS notified federal law enforcement regarding the event. FBCS is also working to implement additional safeguards in a newly built environment. FBCS is providing access to credit monitoring services for twelve (12) months, through Cyex, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, FBCS is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. FBCS is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

FBCS is providing notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A

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

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/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

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/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.