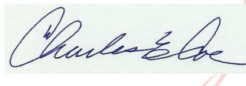




**UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL**

September 26, 2016

TO: James W. Runcie
Chief Operating Officer
Federal Student Aid

FROM: Charles E. Coe, Jr. 
Assistant Inspector General
Information Technology Audits and Computer Crime Investigations

SUBJECT: Final Management Information Report
Misuse of FSA ID and the Personal Authentication Service
Control No. ED-OIG/X21Q0001 (16-220350)

Digitally signed by Charles Coe
DN: c=US, o=U.S. Government, ou=U.S.
Department of Education, cn=Charles Coe,
0.9.2342.19200300.100.1.1=9268225650
Reason: I am approving this document
Date: 2016.09.26 12:45:06 -04'00'

The purpose of this management information report is to inform Federal Student Aid (FSA) of our concerns regarding how the FSA ID and the Personal Authentication Service (PAS) are being misused by commercial third parties to take over borrower accounts. The Office of Inspector General (OIG) has identified this problem through various investigations and has developed recommendations to address the misuse. This report recommends changes to strengthen the banner language for the FSA ID and PAS to enhance the OIG's ability to successfully investigate and prosecute third parties who improperly create, access, or make changes to FSA IDs and accounts. The report also recommends that FSA increase its proactive monitoring of FSA IDs and PAS audit logs and ensure that it proactively monitors the types of abuses identified.

In its August 12, 2016, response to our draft report, FSA did not explicitly agree or disagree with our issues and recommendations and stated that it shares our concerns regarding the growth of fraud and misuse of the FSA ID by third parties. FSA's proposed corrective actions are responsive to many of our recommendations. However, FSA did not provide complete information on some planned corrective actions, and some of the proposed actions are contingent on the results of FSA's further research. We summarize FSA's comments and our responses at the end of each issue and provide the full text of FSA's response as an attachment to this report. We did not make any changes to the issues and recommendations based on FSA's response.

This management information report issued by the Office of Inspector General will be made available to members of the press and general public to the extent information contained in the memorandum is not subject to exemptions in the Freedom of Information Act (5 U.S.C. § 552) or protection under the Privacy Act (5 U.S.C. § 552a).

400 MARYLAND AVENUE, S.W., WASHINGTON, DC 20202-1510

Promoting the efficiency, effectiveness, and integrity of the Department's programs and operations.

FSA TRANSITION FROM PIN TO PAS

Personal Identification Number

Until May 2015, the FSA personal identification number (PIN), a four-digit number used in combination with the user's Social Security number, name, and date of birth, served as an electronic signature and provided access to sensitive personal records on FSA Web sites such as fafsa.ed.gov and pin.ed.gov. The PIN allowed students and their parents the ability to manage their FSA accounts, manage their Free Application for Federal Student Aid (FAFSA), and electronically sign the FAFSA and other related documents. FSA required each person accessing these sites to apply for his or her own PIN. The PIN Web site (pin.ed.gov) instructed users not to share their PIN with anyone and explicitly stated that "you should never give your PIN to anyone, including commercial services that offer to help you complete your FAFSA."

Personal Authentication Service (PAS) for FSA ID Replacing PIN

The FSA ID was implemented in May 2015, to provide a modernized login process and to improve security for FSA Web sites, including FAFSA on the Web, National Student Loan Data System Student Access, StudentLoans.gov, StudentAid.gov, and the TEACH Grant Web site.¹ The FSA ID, which comprises a user-selected username and password, replaced the PIN as the process by which students, parents, and borrowers authenticate their identity to access their Federal student aid information. The PAS (fsaid.ed.gov) is used to generate authentication and log-on credentials for people who want to access FSA Web sites.² FSA's instructions for creating an FSA ID state "Only the owner of the FSA ID should create and use the account. Never share your FSA ID." During the account creation process, the Web site reminds users to only "create an FSA ID using your personal information and for your own exclusive use. You are not authorized to create an FSA ID on behalf of someone else, including a family member." In addition, the applicant agrees to not share his or her FSA ID with anyone and certifies that "under penalty of perjury under the laws of the United States of America that the information I have provided to obtain an FSA ID is true and correct, and that I am the individual who I claim to be. I understand that falsification of this statement may be punishable by a fine, by imprisonment of not more than five years, or both."

¹ Rather than using PAS, financial aid professionals and authorized third parties are required to use FSA's Access and Identity Management System (AIMS) to log in and access FSA's systems, such as Common Origination and Disbursement, FAA Access to CPS Online, National Student Loan Data System Professional Access, and Student Aid Internet Gateway Enrollment. This report specifically addresses third parties improperly accessing PAS by using the loan holder's FSA ID credentials (loan holder username and password) and not third parties who use their own legitimate credentials.

² National Institute of Standards and Technology (NIST) 800-63-2, "Electronic Authentication Guideline," defines electronic authentication as the process of establishing confidence in user identities electronically presented to an information system. For the purposes of the PAS system, a successful authentication occurs when a user logs in using his or her valid FSA ID username and password.

RECURRING ISSUES WITH PIN SECURITY VULNERABILITIES

Past OIG Activities Involving the PIN System and Loan Consolidators

Since 2012, the OIG has investigated several loan consolidation companies that gained access to PIN accounts to consolidate loans or enroll borrowers in debt forgiveness or reduction programs. During 2012, an OIG investigation found that a loan consolidation company charged borrowers a \$45 monthly service fee to consolidate and lower their monthly payments. The loan consolidation company changed the mailing address, phone number, and email address for borrowers so that it would be difficult for the borrowers to be contacted by their loan servicers.³ Another OIG investigation in 2013 also found that a company charged borrowers a \$60 monthly service fee to put their loans into forbearance with the stated promise of eventually enrolling them in the Public Service Loan Forgiveness or some other debt reduction program even though the borrowers, in some cases, were not qualified for these programs. The complainant alleged that the loan consolidation company improperly accessed and changed information in the complainant's PIN account. The OIG investigation found that the loan consolidation company required borrowers to sign a contract and power of attorney that gave the company permission to access their information in the National Student Loan Data System. Ultimately, the execution of the power of attorney impeded the OIG's ability to pursue a criminal charge against the company for unauthorized access to the account.

In the September 2013 OIG management information report, "PIN Security Vulnerabilities," (ED-OIG/X21L0002), the OIG informed FSA that students were sharing their PINs with a company providing loan-related services. The OIG's investigation found that students using the services of this company typed their PINs into the company's Web site so that the company could log in and obtain information on the students' behalf. The OIG reported that this practice may provide an opportunity for bad actors at the company to change and misuse the students' personal data. As a result, the OIG suggested that FSA consider developing a capability to enable students to permit companies providing loan-related services read-only access to relevant areas of their accounts to remove the risk that the company could alter the student's record or obtain the student's sensitive personal information. FSA did not agree with the OIG's suggestion but stated that its deployment of MyStudentData Download met the OIG's objectives for this suggestion. MyStudentData Download, deployed in November 2012 and April 2013, permits students to download a file that includes loan and grant information that students can provide to third parties. FSA stated that it believed no party, other than the student, needed to have direct access (read-only or otherwise) to the student's account information.

³ FSA contracts with entities to manage the servicing of millions of federal student loans. These loan servicers are responsible for advising borrowers on resources and benefits to better manage their federal student loan obligations, responding to customer service inquiries, and performing other administrative tasks associated with maintaining a loan on behalf of the U.S. Department of Education.

In a January 2014 referral memorandum to FSA, “Defunct Loan Consolidation Company Controlling Student Accounts” (13-220017), the OIG informed FSA that 805 PIN user accounts appeared to be controlled by a recently defunct loan consolidation company. The memorandum stated that FSA “should consider taking appropriate actions to contact the students so they can update their email addresses or other contact information to ensure they continue to receive FSA correspondence, and FSA should consider requiring a change to student PINs to preclude abuse.” The memorandum also detailed OIG’s additional analysis to identify similar groups of people with PIN email addresses appearing to belong to a loan consolidation company email address domain. The OIG provided FSA with a list of 12 loan consolidation companies that were potentially controlling PIN user accounts by changing or establishing student email addresses in the PIN system with corporate email addresses. Although the PAS no longer allows people to associate multiple FSA IDs with the same email address, the OIG has found that loan consolidation companies have created FSA IDs that are associated with corporate email address domains. Corporate email servers allow the companies to intercept all of the borrower’s email correspondence, including password resets via email, important email notices, and direct communication from FSA or the loan servicer.

Current OIG Activities Involving the PAS System and Loan Consolidators

Most recently in September 2015, the OIG investigated whether one or more U.S.-based entities were perpetrating a possible fraudulent scheme by offering questionable student loan consolidation or forgiveness services to people with current student loans. The OIG investigated the allegation that the perpetrators were controlling many accounts by illegally creating, accessing, and changing FSA ID logon information, which could lock out the borrowers. During interviews, the victim borrowers stated that over a period of weeks, they would receive daily calls from a call center, and that the callers were overly aggressive in trying to get the borrowers to provide their account and loan information.

The OIG identified 10,849 FSA IDs associated with six IP addresses used by a third party in India from May through November 2015. The OIG analyzed the PAS audit logs to identify the specific activity associated with these FSA IDs when the transaction originated from the IP address used by the third party. The OIG found that 45 percent of these transactions resulted in a successful authentication allowing access into the borrower’s account. In addition, the OIG found that 22 percent of the transactions were associated with a successful username and password reset that was provided via email and that 19 percent of the transactions were associated with a new FSA ID account creation.

However, the OIG closed the complaint due to the challenges of criminally prosecuting the third party: in many instances, even though it did not have authorization from FSA to access borrower accounts, the third party had nonetheless obtained consent from the borrowers to access their accounts. The OIG determined that because the current banner language for the FSA ID and PAS does not explicitly prohibit third-party access, it would be difficult to successfully pursue a criminal prosecution for unauthorized access against a third party who accesses a user’s account with the user’s permission—even in cases where the third party accessed the account for the purposes of commercial advantage or private financial gain.

During the investigation, the OIG met with FSA staff to suggest improvements to the banner language for the FSA ID and PAS.

ISSUE 1 – BANNER AND INSTRUCTIONS INADEQUATE TO PREVENT COMMERCIAL THIRD-PARTY ACCESS TO FSA ID AND PAS

The OIG has determined that the current instruction language used in the FSA ID creation process and the banner used in FSA system log on are not adequate to establish that a third party's access to PAS with an authorized user's FSA ID constitutes criminal unauthorized access as defined by 18 U.S.C. § 1030.

FSA ID Account Creation Process

On the first page of the FSA ID creation Web page, the user is instructed that "You are not authorized to create an FSA ID on behalf of someone else, including a family member. Misrepresentation of your identify to the federal government could result in criminal or civil penalties." In addition, the following unauthorized access warning banner appears at the bottom of the Web page in small, italicized print:

This is a U.S. Federal Government owned computer system, for the use by authorized users only. Unauthorized access violates Title 18, U.S. Code Section 1030 and other applicable statutes. Violations are punishable by civil and criminal penalties. Use of this system implies consent to have all activities on this system monitored and recorded, which can be provided as evidence to law enforcement officials.

On the second page, the user is instructed that he or she will "be required to certify that the information that I provide to obtain an FSA ID is true and correct and that I am the individual who I claim to be. If I am not that person who I claim to be, I understand that I am not authorized to proceed and that I should exit this form now. If I provide false or misleading information, I understand that I may be fined, sent to prison for not more than five years, or both." The user provides identifying information on pages two through four and establishes challenge questions and answers on the fifth page.

On the sixth page, the user reviews his or her FSA ID application information and the following terms and conditions for the FSA ID:

Read before you proceed.

By submitting this application, you agree not to share your FSA ID with anyone. The security of your FSA ID is important because it can be used to

- electronically sign Federal Student Aid documents
- access your personal records, and
- make binding legal obligations.

If your FSA ID is lost or stolen, you also agree to

- contact Federal Student Aid's Customer Service center at 1-800-4-FED-AID (1-800-433-3243)
- change your password by selecting Change My Password under the Edit My FSA ID tab, or
- disable your FSA ID so that no one can use it by selecting Disable My FSA ID under the Edit My FSA ID tab.

I declare under penalty of perjury under the laws of the United States of America that the information I have provided to obtain an FSA ID is true and correct, and that I am the individual who I claim to be. I understand that falsification of this statement may be punishable by a fine, by imprisonment of not more than five years, or both.

If you agree to these terms, select the “I certify that the above information is correct & accept the terms & conditions.”

If you do not agree to the conditions, select CANCEL.

The user must check a box stating that, “I certify that the above information is correct & accept the terms & conditions” before he or she can click “continue” to take steps to finish applying for an FSA ID.

The OIG has determined that the terms and conditions could be strengthened to directly address third parties who create FSA IDs. Although the instructions prohibit the creation of an FSA ID for someone else, and the terms and conditions prohibit a user from sharing his or her FSA ID, they do not directly address third-party access to FSA IDs. The instructions also do not establish that subsequent access to FSA systems by a third party using a user’s FSA ID constitutes unauthorized access.

FSA ID/PAS Logon

Another banner is encountered each time the FSA ID is used to log on to a system using PAS.⁴ The unauthorized access banner is at the bottom of the Web page in small, italicized print, and the user does not have to take any action to acknowledge or agree to the warning banner. Also, the banner language does not specifically prohibit third-party access. This banner reads:

This is a U.S. Federal Government owned computer system, for the use by authorized users only. Unauthorized access violates Title 18, U.S. Code Section 1030 and other applicable statutes. Violations are punishable by civil and criminal penalties. Use of this system implies consent to have all activities on this system monitored and recorded, which can be provided as evidence to law enforcement officials.

⁴ PAS is used to generate authentication and log-on credentials for individuals accessing their personal records including the following FSA systems: Free Application for Federal Student Aid, studentaid.ed.gov, StudentLoans.gov, TEACH Grant to Serve, Federal Student Aid Information Center, and the National Student Loan Data System Student Access.

Improvements to Banner Language

The OIG has determined that more explicit language is needed to put third parties—in particular, predatory loan consolidators accessing the system for purposes of commercial advantage or private financial gain—on notice that their access is unauthorized. Unauthorized access of protected systems for the purposes of commercial advantage or private financial gain is prohibited by 18 U.S.C. § 1030 (Fraud and Related Activity In Connection With Computers).

In December 2015, OIG and PAS staff discussed adding logon banner language that specifically addressed unauthorized third-party users. The OIG suggested that a pop up could occur after the user enters their correct credentials and pushes the button to log in, as successfully demonstrated by another Federal Agency. PAS staff expressed several technical concerns with a login pop up and instead suggested that users be taken to a second screen, after entering correct credentials, where they would accept the terms of service before accessing protected applications. FSA proposed a click-through solution that prevents further activity on the system unless a user executes a positive action, such as clicking on a box indicating “OK.” The OIG suggested the following banner language that could be used with either a pop up or click-through solution:

This is a U.S. Federal Government computer system intended to be accessed solely by individual users expressly authorized to access the system by the U.S. Department of Education. For security purposes and to ensure that the system remains available to all expressly authorized users, the U.S. Department of Education monitors the system to identify unauthorized users. Anyone using this system expressly consents to such monitoring. Except as expressly authorized by the U.S. Department of Education, unauthorized attempts to access, obtain, upload, modify, change, and/or delete information on this system are strictly prohibited and are subject to criminal prosecution under 18 U.S.C. § 1030, and other applicable statutes, which may result in fines and imprisonment. **For purposes of this system, unauthorized access includes, but is not limited to:**

-Any access by an employee or agent of a commercial entity, or other third party, who is not the individual authorized user, for purposes of commercial advantage or private financial gain (regardless of whether that commercial entity or third party is providing a service to an authorized user of the system); and

-Any access in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

If system monitoring reveals information indicating possible criminal activity, such evidence may be provided to law enforcement personnel.

This language is based directly on 18 U.S.C. § 1030 and would unambiguously put third parties on notice that their access is subject to prosecution under that statute. However, the Department informed the OIG in January 2016 that it would not implement a logon banner in favor of alternative remedies such as issuing cease and desist letters. In the OIG’s view, cease and desist letters are an ineffective remedy because they serve only to attempt to prevent future access. The letters do not allow the potential criminal prosecution of past illegal use of

the system. Although FSA can take steps to block the commercial third party's IP address and disable user accounts that were created or updated by the commercial third party, those actions will not act as a deterrent to other companies conducting the same type of illegal activity. Further, this reliance on cease and desist letters prohibits the Department from obtaining any restitution or fines for the illegal activity.⁵

RECOMMENDATIONS

We recommend that the Chief Operating Officer for FSA:

- 1.1 Revise the terms and conditions in the FSA ID account creation process to specifically address unauthorized access by commercial third-party users.
- 1.2 Revise the plain language instructions in the FSA ID account creation process to warn about predatory third-party debt relief companies that request a person's FSA ID.
- 1.3 Revise the PAS logon banner for the FSA ID to reflect the suggested banner language concerning unauthorized access. FSA should use a "click-through" or "pop up" so the user would have to take an overt action to consent to monitoring and could not say that they did not see the language before logging into an FSA system.

FSA RESPONSE

Response to OIG Recommendations 1.1 and 1.2

FSA stated that it appreciates that revising the terms and conditions of the FSA ID account creation process to address specifically unauthorized access by commercial third-party users will support criminal investigations and other enforcement actions against such third-party users. Noting that the FSA ID account creation process is used over 180 million times a year to authenticate users accessing FSA's systems, FSA stated that "even a small change will likely have a significant impact on third-party users lawfully accessing our systems, including student financial aid application preparers, high school counselors, and non-governmental organizations who work with disadvantaged populations to access financial aid."⁶

⁵ On March 30, 2016, FSA issued an electronic announcement on its Information for Financial Aid Professionals Web site advising schools to provide warnings to students about third-party companies, including that student loan borrowers should avoid demands to sign a third-party authorization or requests for a student's FSA ID. Although this puts schools on notice that they need to warn students about predatory third party companies, FSA should also provide notice to the students to protect the integrity of transactions using PAS.

⁶ FSA provided the following clarification on September 1, 2016: "FSA's reference to 'third-party users lawfully accessing our systems' was intended to speak to situations where a disabled individual, for example, may require a professional's help to physically create an FSA ID or logon to a system. FSA does not support anyone other than the authorized user of the account using the credentials to access their account information. The sharing of credentials is forbidden under our existing policy and all of our materials state that only the owner of the FSA ID

FSA is working with the White House's United States Digital Services to review the processes to create and login to FSA ID; as part of this work, FSA is reviewing the OIG banner recommendation. When it concludes this work, FSA will implement changes consistent with the OIG's recommendations.

Response to OIG Recommendation 1.3

FSA stated that after discussions with the United States Digital Services, the Office of General Counsel, and the OIG, FSA will add appropriate warning language to the login process for all systems using the FSA ID. It will add the language to the login processes for PAS, Studentloans.gov, FAFSA on the Web, studentaid.ed.gov, and TEACH Grant Web site.

OIG RESPONSE

FSA's planned corrective actions for Recommendations 1.1 and 1.3, if implemented, are responsive to our recommendations. If FSA changes the banner language that we recommend in an effort to allow legitimate third party access, the change should clearly prohibit unauthorized access by predatory commercial third parties. Such warnings are necessary to protect borrowers from sharing their FSA IDs with predatory commercial third parties who gain financially from this access and often obtain the access through questionable means. When a third party takes control of a borrower's account, the borrower's personally identifiable information may be put at risk, and the third-party company may maintain access to the borrower's account even when the third party no longer needs access.

FSA's response did not specify a corrective action for Recommendation 1.2 concerning incorporating warnings to users about predatory third party debt relief companies requesting a person's FSA ID.

ISSUE 2 – PAS AUDIT LOG PROACTIVE MONITORING COULD BE IMPROVED

FSA could improve proactive monitoring of the PAS audit logs to identify suspicious activities and report those activities to the Department's Computer Incident Response Capability and the OIG.

FSA Analysis of PAS Logs and Identification of Suspicious Activities

In December 2015, FSA identified that an IP address, associated with a third-party company in India, was used to successfully authenticate in PAS and access information for 4,797 user accounts. PAS staff provided the OIG with this data in furtherance of the September 2015 OIG investigation of the same third-party company that was pressuring borrowers to provide their PAS usernames and passwords. In January 2016, FSA generated a Suspicious Event Report

should create one or use it to login. However, we don't want to discourage individuals such as parents, financial aid counselors, and college counselors from assisting applicants and borrowers, who need assistance to logon or create an FSA ID. Therefore, FSA thinks we need to consider these situations when making changes."

regarding a loan consolidator. The IP address registered to the loan consolidator was associated with 13,400 unique FSA IDs. FSA also found that 8,260 account creation transactions originated from this IP address. FSA subsequently blocked the IP address and disabled all user accounts that were created or updated by the loan consolidator.

Although PAS staff identified suspicious activity and reported it to appropriate Department and OIG officials, they stated that they can do very little analysis of the PAS logs in real time and that only one employee is involved in analyzing PAS trends. PAS staff added that they have a difficult time differentiating legitimate user activity from unauthorized third-party activity. PAS staff also informed the OIG of a limitation in the PAS audit logs. The PAS audit logs note only the date, time, and IP address associated with an account change. The PAS audit logs do not retain or capture a user's previous mailing address, phone number, or email address if that information is changed. Therefore, a user's original contact information could be lost in the system if a third party changes that information.

OIG Proactive Analyses of Third-Party Abuse

In response to the September 2015 complaint to the OIG, the OIG conducted proactive analysis of records in PAS to identify suspicious trends related to IP addresses. First, the OIG identified IP addresses associated with more than 1,000 successful authentications between May 10, 2015, and November 30, 2015. The top IP address was associated with as many as 66,660 distinct account authentications. The top 15 IP address registrants included debtpaypro.com, Intuit Inc., Amazon Technologies, Lauderdale Marina,⁷ and Rubber Chicken Cards.⁸ Second, the OIG identified the top 10 IP addresses associated with the most account creations between May 10, 2015, and November 30, 2015. The top IP address was associated with about 31,000 distinct account creations. The top 10 IP address registrants included various Internet service providers, ITT Educational Service, and Lauderdale Marina.

The OIG identified FSA ID accounts using email address domains appearing to belong to loan consolidation companies.⁹ The OIG specifically analyzed two debt consolidation companies that were each associated with more than 2,000 FSA IDs.

⁷ This IP address is associated with 36,522 FSA IDs and appears to be registered to a marina located in Florida and does not appear to be associated with a company or organization involved in higher education or student loans. The OIG found that more than 6,000 FSA IDs were associated with the same password.

⁸ This IP address is associated with 13,775 FSA IDs and appears to be registered to an e-card company located in California and does not appear to be associated with a company or organization involved in higher education or student loans. The OIG found that more than 8,000 FSA IDs were associated with the same password.

⁹ The OIG previously reported in the September 2011 investigative program advisory report, "Distance Education Fraud Rings" (L42L0001), that single email addresses were used to receive and manage PIN accounts for hundreds of people. In the September 2013 management information report, "PIN Security Vulnerabilities" (ED-OIG/X21L0002), the OIG reported that students were sharing their PINs with a third-party company providing loan services, which provides an opportunity for bad actors at the company to change and misuse the student's personal data.

The OIG found that 2,800 FSA IDs had an email address ending in the domain @1file.org, which is used by 1file.org, which is also known as Student Loan Processing. The OIG found the following similarities for the 2,800 FSA IDs:

- 1) 2,508 accounts established the same significant date for the user (the FSA ID instructions tell users to enter a significant date in their lives): [REDACTED]
- 2) 2,160 accounts had the same four challenge questions and answers: [REDACTED]
[REDACTED]
[REDACTED]
- 3) 1,938 accounts were associated with the same IP address.
- 4) 104 groups of borrowers, ranging from 10 to 40 people in each group, shared the same passwords.

The OIG also found that 2,764 FSA IDs had an email address ending in the domain @unitedadvisorsgroup.com, which is used by the United Advisors Group, which provides debt consolidation services. The OIG found the following similarities for the 2,764 FSA IDs:

- 1) 2,736 accounts had the same current or previous password.
- 2) 2,707 accounts had the same two challenge questions and answers: [REDACTED]
[REDACTED]
[REDACTED]
- 3) 2,317 accounts were created from the same IP address.

All of the similarities noted by the OIG in its own analysis show potential suspicious activities that may warrant further action. It is important for FSA to conduct similar monitoring and trend analyses on an ongoing basis to identify potential misuse of FSA IDs, which may indicate borrowers who are at risk of predatory practices. FSA needs to continue improving how it identifies third-party companies that take control of borrower accounts. Such control may put borrowers' personally identifiable information at risk and provide routine access to the borrower's account and information even when the third-party companies no longer need access. In addition, when third-party companies create accounts on behalf of borrowers or change account information, FSA and loan servicers may not be able to contact the borrower (because the phone number or email address may be compromised) and the borrower may no longer be able to access his or her account.

In addition, these third-party companies are violating the user agreement and intended purpose of the system by creating, accessing, and/or changing FSA ID accounts. Third-party companies need to be informed explicitly that it is a violation of 18 U.S.C. § 1030 for them to access a person's Federal student account or record using a FSA ID assigned to a borrower. Putting third-party companies on explicit notice will provide strong evidence for prosecution and also function as a deterrent.

RECOMMENDATIONS

We recommend that the Chief Operating Officer for FSA:

- 2.1 Implement a proactive monitoring schedule to analyze trends related to FSA ID accounts and transactions including account creations, logons, and changes; and report any suspicious activity to the Department of Education's Computer Incident Response Capability and the OIG.
- 2.2 Take appropriate administrative action against companies or individuals that are abusing or misusing the terms and conditions for the FSA ID.
- 2.3 Enable the PAS audit logs to retain previous account information or values before a user updates his or her FSA ID account.

FSA RESPONSE

Response to OIG Recommendation 2.1

FSA will conduct pattern analysis of various audit events and user data. However, FSA's analysis is limited based on the encryption techniques FSA employed to better align with commercial best practices and as recommended by United States Digital Services.

Response to OIG Recommendation 2.2

FSA will take appropriate administrative action against companies or individuals that are abusing or misusing the terms and conditions of the FSA ID. This may include shutting down unlawful access, referring cases to the OIG, locking user accounts, blocking Internet Service Providers, and referring individuals to other agencies for legal action. FSA will consult with Federal consumer protection agencies, such as the Consumer Financial Protection Bureau and the Federal Trade Commission, to determine whether these agencies might be able to take action against companies and individuals that abuse or misuse the FSA ID.

Response to OIG Recommendation 2.3

FSA will enable the PAS audit logs to retain previous account information or values before the user updates his or her FSA ID account.

OIG RESPONSE

FSA's planned corrective actions for Recommendations 2.1, 2.2, and 2.3, if implemented, are generally responsive to our recommendations. With regard to Recommendation 2.1, FSA did not specify if it would report suspicious activity to the Department of Education's Computer Incident Response Capability and the OIG. With regard to Recommendation 2.2, we understand that encryption techniques were implemented due to United States Digital Services recommendations and that encryption provides challenges for proactive analysis, but we encourage FSA to use pattern analysis or metadata analysis solutions for the encrypted data elements.

OBJECTIVE, SCOPE, AND METHODOLOGY

On January 25, 2016, the OIG opened a proactive investigative project. The objective of this project was to analyze FSA IDs and PAS logs and to communicate security shortcomings to FSA. To answer the objective, the OIG limited its analysis to data available from May 10, 2015, through November 30, 2015. The OIG analyzed PAS Audit log and PAS FSA ID account information tables for suspicious trends related to loan consolidation companies. Specifically, the OIG analyzed trends related to IP addresses, email address domains, passwords, and challenge question and answers. The OIG also analyzed the PAS audit logs to identify what commercial third parties were doing with the borrower's account once the FSA ID was created.

The OIG initiated this project in response to the September 2015 complaint to the OIG, in which the OIG investigated whether U.S.-based entities were perpetrating a fraudulent scheme by offering loan consolidation or forgiveness services to people who currently hold Federal student loans. Based on victim interviews, the OIG determined that possible third-party entities telephoned borrowers to persuade them to reveal their FSA ID credentials for PAS for the purposes of completing a student loan consolidation transaction.

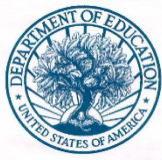
The OIG provided a draft of this report to FSA on June 30, 2016. FSA provided its response to the draft report on August 12, 2016. In response to a question from the OIG, FSA provided a clarification to the language on September 1, 2016. We included FSA's response as an attachment to this report.

The OIG conducted its work in Washington, DC from December 2015 through June 2016 in accordance with the Council of the Inspectors General on Integrity and Efficiency, Quality Standards for Inspection and Evaluation.

This management information report issued by the Office of Inspector General will be made available to members of the press and general public to the extent information contained in the report is not subject to exemptions in the Freedom of Information Act (5 U.S.C. § 552) or protection under the Privacy Act (5 U.S.C. § 552a).

If you have any questions, please contact Robert D. Mancuso, Special Agent in Charge, Technology Crimes Division, at (202) 245-7330.

cc: Ted Mitchell, Under Secretary, U.S. Department of Education
Dawn Dawson, Audit Liaison Officer, FSA
Jeff Baker, Director, Policy Liaison and Implementation, FSA
William Leith, Chief Business Operations Officer, FSA
Keith Wilson, Chief Information Officer, FSA
Ganesh Reddy, PAS System Owner, FSA



UNITED STATES DEPARTMENT OF EDUCATION

Federal Student Aid

August 12, 2016

TO: Charles E. Coe, Jr.
Assistant Inspector General
Information Technology Audits and Computer Crime Investigations

FROM: James W. Runcie
Chief Operating Officer

SUBJECT: Draft Management Information Report, "Misuse of FSA ID and the Personal Authentication Service"
Control No. ED-OIG/X21Q0001 (16-220350)

Thank you for providing Federal Student Aid (FSA) with an opportunity to respond to the Office of Inspector General's (OIG) draft Management Information Report entitled, "Misuse of FSA ID and the Personal Authentication Service." Your report recommends changes to strengthen the banner language for the FSA ID and Personal Authentication Service (PAS), and to increase monitoring of the FSA ID and PAS audit logs.

We share your concerns regarding the growth of fraud and the misuse of the FSA ID by third parties. As you know, we are currently working with the United States Digital Services (USDS) to review the FSA ID creation and login process, and reviewing OIG's suggestions is a part of that work.

We have responded to each of your specific recommendations below:

ISSUE 1—BANNERS INADEQUATE TO PREVENT COMMERCIAL THIRD-PARTY ACCESS TO FSA ID AND PAS

- 1.1 Revise the terms and conditions in the FSA ID account creation process to specifically address unauthorized access by commercial third-party users.
- 1.2 Revise the plain language instructions in the FSA ID account creation process to warn about predatory third-party relief companies that request a person's FSA ID.

Response to 1.1 and 1.2: We appreciate that revising the terms and conditions of the FSA ID account creation process to address specifically unauthorized access by commercial third-party users will support criminal investigations and other enforcement actions against third-party users violating 18 U.S.C. § 1030. However, the FSA ID account creation process is used over 180 million times a year to authenticate users accessing FSA's systems. As such, even a small change will likely have a significant impact on third-party users lawfully accessing our systems, including student financial aid application preparers, high school counselors, and non-governmental organizations who work with disadvantaged populations to access financial aid.

Accordingly, FSA needs to understand the usability and operational impacts of this recommended change. FSA is currently working with the White House's USDS to review the processes to create and login to FSA ID; as part of that work, we are reviewing the OIG banner recommendation so that users will have to take an overt action to consent to monitoring and could not say that they did not see the language before logging into an FSA system. Upon the conclusion of this field work and research, FSA will implement changes consistent with the OIG's recommendations.

1.3 Revise the PAS logon banner for the FSA ID to reflect the suggested banner language concerning unauthorized access. FSA should use a "click-through" or "pop up" so the user would have to take an overt action to consent to monitoring and could not say that they did not see the language before logging into an FSA system.

Response: FSA will add additional warning language to the login process for all systems using the FSA ID. This language will be added after discussions with USDS, the Office of the General Counsel and the OIG on the most appropriate wording which will address the concerns about unauthorized access and address concerns about the impact to FSA's 36 million users. Once the language is agreed upon, FSA will test the login with users and then deploy the final changes. The new language will be added to the FSA ID/PAS, Studentloans.gov, FAFSA, StudentAid.gov and ATS/TEACH login processes.

ISSUE 2—PAS AUDIT LOG PROACTIVE MONITORING COULD BE IMPROVED

2.1 Implement a proactive monitoring schedule to analyze trends related to FSA ID accounts and transactions including account creations, logons, and changes; and report any suspicious activity to the Department of Education's Computer Incident Response Capability and the OIG.

Response: FSA will begin conducting pattern analysis of various audit events and user data including user created challenge questions, IP addresses of organizations, email address domain names, HTTP header information and transaction types for PAS. However, our analysis is limited based on the encryption techniques FSA recently employed to better align with commercial best practices and as recommended by USDS.

2.2 Take appropriate administrative action against companies or individuals that are abusing or misusing the terms and conditions for the FSA ID.

Response: FSA will take appropriate administrative action against companies or individuals that are abusing or misusing the terms and conditions of the FSA ID. This may include shutting down unlawful access and referring cases to the OIG, locking user accounts, blocking ISPs, along with referring individuals to the appropriate other agencies for legal action. FSA will consult with federal consumer protection agencies, such as the Consumer Financial Protection Bureau and the Federal Trade Commission, to determine if these agencies might be able to take action against companies and individuals that abuse or misuse the FSA ID.

2.3 Enable the PAS audit logs to retain previous account information or values before a user updates his or her FSA ID account.

Response: FSA will enable the PAS audit logs to retain previous account information or values before user updates his or her FSA ID account.

FSA appreciated the opportunity to respond to your recommendations, and we look forward to further discussions with OIG on this important subject.

cc: Robert Mancuso, Special Agent-in-Charge, Technology Crimes Division
Ted Mitchell, Under Secretary, U.S. Department of Education