

[PUBLISH]

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

No. 09-15295

FILED U.S. COURT OF APPEALS ELEVENTH CIRCUIT AUGUST 11, 2011 JOHN LEY CLERK
--

D. C. Docket No. 08-00050-CR-4-SPM-WCS

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

versus

MARCUS BARRINGTON,

Defendant-Appellant.

Appeal from the United States District Court
for the Northern District of Florida

(August 11, 2011)

Before HULL and MARCUS, Circuit Judges, and WHITTEMORE,* District Judge.

WHITTEMORE, District Judge:

* Honorable James D. Whittemore, United States District Judge, Middle District of Florida,
sitting by designation.

Marcus Barrington appeals his convictions for conspiracy to commit wire fraud using a protected computer, accessing a protected computer without authorization with intent to defraud, and three counts of aggravated identity theft. Barrington also appeals his sentence, contending that his 84 month prison sentence is procedurally and substantively unreasonable.¹

Barrington challenges the admission of Rule 404(b) evidence at trial, the district court's restriction on cross-examination of a cooperating co-defendant, and the sufficiency of the evidence supporting his aggravated identity theft convictions. Additionally, he contends the conspiracy count in the indictment was duplicative and the jury instructions on conspiracy and aggravated identity theft were erroneous.

As for his sentence, he contends that the district court erred in calculating his base offense level, infringed on his right against self-incrimination at sentencing, erred in calculating loss, and erred in applying Guidelines enhancements for use of sophisticated means, leadership role, device-making equipment, and production of unauthorized access devices.

¹ Barrington was sentenced to concurrent 60 month terms on the conspiracy and fraud counts and 24 month terms on the three counts of aggravated identity theft, concurrent with each other but consecutive to the 60 month terms on the conspiracy and fraud counts. His 84 month sentence was within the advisory Guidelines range as to Counts 1 and 2, and statutorily mandated as to Counts 3, 4, and 5.

For the reasons discussed below, we affirm Barrington's convictions and sentence.

I

Barrington and his co-defendants, Christopher Jacquette and Lawrence Secrease, all undergraduate students at Florida A&M University ("FAMU"), were indicted and charged in a five count indictment with conspiracy to commit wire fraud using a protected computer in violation of 18 U.S.C. §§ 371 and 1349; fraud using a protected computer in violation of 18 U.S.C. §§1030(a)(4) and (c)(3)(A) and 2; and three counts of aggravated identity theft in violation of 18 U.S.C. §§ 1028A and 2. Jacquette and Secrease pleaded guilty pursuant to plea agreements, received substantial assistance departures pursuant to U.S.S.G. § 5K1.1, and were each sentenced to 22 months in prison and 3 year terms of supervised release.

The offense conduct

Barrington's convictions arose from a scheme he and his co-conspirators concocted to access FAMU's internet-based grading system. The scheme was developed after Secrease and Barrington, roommates at the time, began discussing how to change grades for friends who were applying to graduate school. During the summer of 2007, Barrington changed grades for himself, Jacquette and several

fraternity brothers using forged University grade change slips. When that method became ineffective in part because they ran out of blank grade change slips, they developed a plan to access the system using keylogger software.²

Secrease was with Barrington in the Registrar's Office in August 2007 when they attempted to install the first keylogger. They eventually installed keylogger software on various University computers, including an office computer used by a Registrar employee and four terminals placed in the University's grand ballroom during registration. The keyloggers covertly recorded the keystrokes made by Registrar employees as they signed onto their computers, capturing their usernames and passwords. That data was automatically transmitted to various email accounts, including Barrington's personal email address.

Using the surreptitiously obtained usernames and passwords, the conspirators accessed FAMU's grading system, changed grades, added credits for courses which had been failed or not taken, and changed the residencies of several non-resident students to qualify them for in-state tuition.³ The changes were made

² A keylogger, also referred to as a keystroke logger, captures every key depression, or keystroke, made on a computer. *PCMAG.com*. "Keylogging," the practice of covertly recording and monitoring keystrokes made on a computer, is typically accomplished through use of a dedicated software application or piece of implanted hardware. *Collins English Dictionary, Unabridged (10th ed. 2009)*.

³ For example, in September 2007, twin sisters who were non-resident students paid \$1200 to have their residencies changed. Jacquette negotiated the agreement, Secrease transmitted their information to Barrington, and Barrington effected the change. The three of

via the Internet from the conspirators' home computers, campus computers at FAMU and Florida State University, and from several wireless laptops.

A joint investigation by FAMU's Police Department and the FBI determined that FAMU's protected grading system had been accessed by unauthorized means. The investigation was triggered after a FAMU professor discovered that one of his students, Barrington's sister, had received two unauthorized grade changes. The University subsequently discovered that between August and October 2007, approximately 30 to 35 unauthorized changes were made to Barrington's grades, all but one from a lower grade to an A. Barrington's sister received 5 grade changes from F or C to A. Jacquette received approximately 43 grade changes and Secrease received approximately 36. Ultimately, the investigation revealed that in excess of 650 unauthorized grade changes had been made, involving at least 90 students. As a result of the grade changes and residency changes, the University incurred a loss of \$137,000 in tuition it otherwise would have received.

In September 2007, Barrington and his sister were questioned by FAMU police. Barrington denied any knowledge of the grade changes. Within hours, and after learning that the University had reversed the grade changes, Barrington

them split the \$1200. Jonathan Huggs and Secrease had their residencies changed as well. Huggs received a tuition reimbursement and Secrease received a 75% refund totaling \$15,000-\$20,000. Non-resident students paid approximately four times the tuition in-state students paid.

organized a meeting at his house with Jacquette, Secrease, and some of the students whose grades had been changed. Barrington instructed them to deny all knowledge of the scheme if questioned by police. They agreed to re-install keyloggers on the Registrar's computers so that the grades could be changed a second time. Barrington drew a map and directed students where to go to carry out the plan. Some of them went to the Registrar's Office where they distracted employees so that others could install keyloggers using flash drive devices. Afterwards, the group celebrated at a local Chili's restaurant.

At some point, Secrease was terminated from his job at the University, losing access to the University's computer lab. Barrington provided funds to Jacquette for the purchase of a laptop computer. Notwithstanding that law enforcement had discovered the scheme and the University was reversing the grade changes, the conspirators continued to make grade changes using the laptop.

In an effort to conceal their involvement, the conspirators made random grade changes for students who had not been involved originally. Jacquette explained that this was done to "throw things off by broadening the list of names" of students whose grades had been changed. Barrington told Jacquette that random grade changes would indicate that either there was a "flaw or hiccup" in the computer system, or that another group of students was responsible. According to

Jacquette, Barrington's "logic was, if grade changes continue[d], there [was] no way the police would think that [he did it because] he had to be an absolute idiot to continue doing it after they've already contacted him. But if it continued, they would think that it must be someone else."

In November 2007, search warrants were executed at the conspirators' residences, resulting in the seizure of documents containing the usernames and passwords of seven FAMU Registrar employees, handwritten notes outlining classes and grades and directing certain grade changes, FAMU student transcripts, restricted student enrollment documents, and student class information and ID numbers. In Barrington's room, the officers found an index card with usernames and passwords of Registrar employees written on it. They did not find the laptop that had been used to make the grade and residency changes. It was later determined that Barrington had taken it for safekeeping to the home of another student, who ultimately turned it over to the police. An analysis of the laptop confirmed that it had been used to effect grade and residency changes.

Jacquette consented to a search of his cell phone. On his phone were the usernames and passwords of several Registrar employees. Jacquette testified that this information came from an index card written by Barrington.

Barrington testified at trial. He essentially denied any involvement in the

scheme, claiming that he was merely present during the installation of the keyloggers, the grade changing and the concealment activities. In rebuttal, an FBI agent who took Barrington's Rule 11 proffer testified that Barrington admitted to having participated in the scheme to obtain the usernames and passwords, acting as a lookout while Secrease and Jacquette installed the keyloggers on Registrar computers, having used the passwords, and having asking to have his sister's and another female student's grades changed. The Government also called Sheerie Edwards, a friend of Barrington's. She testified that after discussing with Barrington that she had not done well in certain classes, he told her that her grades could be "fixed." She gave him a list of the classes. Later, Barrington called her and told her to look at her grades online. When she did, she saw that her grades had been changed.

Barrington was convicted on all counts.

II

Barrington first contends that the district court erred in admitting into evidence testimony from Jacquette describing how Barrington had previously changed grades using forged instructor signatures on University grade change slips. Barrington contends that this testimony was inadmissible under Fed. R. Evid. 404(b). We disagree. Such rulings are reviewed for abuse of discretion. *See*

United States v. Jernigan, 341 F.3d 1273, 1280 (11th Cir. 2003); *United States v. West*, 898 F.2d 1493, 1499 (11th Cir. 1990).

Prior to trial, the Government filed a notice of its intent to introduce testimony that Barrington had fraudulently changed student grades by “forging legitimate student grade change forms and submitting them for processing.” Barrington objected and before Jacquette testified, the district court considered the Government’s proffer of the challenged evidence. It found that the evidence was relevant to Barrington’s intent, that Jacquette’s testimony sufficiently established that Barrington had engaged in the activity, and that the probative value was not outweighed by unfair prejudice.

Extrinsic evidence of prior bad acts is admissible under Rule 404(b) to show, among other things, motive, preparation, knowledge, and intent. *United States v. Perez*, 443 F.3d 772, 779 (11th Cir. 2006). Rule 404(b) evidence, “like other relevant evidence, should not lightly be excluded when it is central to the prosecution’s case.” *Jernigan*, 341 F.3d at 1280 (quoting *United States v. Perez-Tosta*, 36 F.3d 1552, 1562 (11th Cir. 1994)). A three step test is applied in determining the admissibility of extrinsic 404(b) evidence: (1) the evidence must be relevant to an issue other than the defendant's character; (2) there must be sufficient proof so that the jury could find that the defendant committed the

extrinsic act; and (3) the evidence must possess probative value that is not substantially outweighed by undue prejudice. *Id.*

By pleading not guilty, Barrington placed his intent to participate in the grade changing scheme in issue. *See United States v. Edouard*, 485 F.3d 1324, 1345 (11th Cir. 2007). The Government could accordingly introduce qualifying 404(b) extrinsic act evidence to prove intent. *Id.* And because he raised the “mere presence” defense, qualifying extrinsic act evidence became “highly probative.” *United States v. Delgado*, 56 F.3d 1357, 1366 (11th Cir. 1995).

Where extrinsic act evidence is offered to prove intent, “its relevance is determined by comparing the defendant’s state of mind in perpetrating both the extrinsic and charged offenses.” *United States v. Dorsey*, 819 F.2d 1055, 1060 (11th Cir. 1987). Where, as here, the state of mind required for the charged offense and the extrinsic act is identical, the first prong of the Rule 404(b) test is satisfied. *Id.*

According to Jacquette, in the summer of 2007, the subject of changing grades came up in a discussion with Barrington. Legitimate but blank University grade change slips were filled out with the student’s information, class, and grade to be changed. The instructor’s and chairman’s signatures were forged, and the form was submitted to the Dean’s office for processing by the Registrar’s office.

Barrington changed two or three of his own grades, Jacquette's Economics grade, and a "couple of more" for fraternity brothers.

This grade changing activity was essentially a precursor to the charged scheme. One reason Barrington switched from hard copy forgery of the grade change slips to the keylogger scheme was that a grade change for his sister Mia had been rejected. Barrington explained to Jacquette that the forms were numbered and he could not obtain any additional slips. Subsequent discussions led to the idea of using passwords of Registrar employees to access the University's system to change grades. When their effort to obtain passwords by "eyeballing" the employees failed, Jacquette mentioned the use of keylogger programs, which eventually became the operational method of the charged scheme.

Jacquette's testimony describing Barrington's grade changing through forgery was properly admitted under Rule 404(b). First, both the extrinsic and charged conduct involved the same intent. Barrington's conduct was therefore highly probative of his intent to participate in the charged scheme. Second, there was an adequate basis for the jury to find that Barrington actually committed the extrinsic acts. Jacquette's uncorroborated testimony was sufficient, since he had personal knowledge of Barrington's conduct. *United States v. Duran*, 596 F.3d 1283, 1298 (11th Cir. 2010) (citing *United States v. Dickerson*, 248 F.3d 1036,

1047 (11th Cir. 2001); *United States v. Bowe*, 221 F.3d 1183, 1192 (11th Cir. 2000) (“In this circuit, the uncorroborated word of an accomplice . . . provides a sufficient basis for concluding that the defendant committed extrinsic acts admissible under Rule 404(b).”), *cert. denied*, 131 S. Ct. 210 (2010).

Finally, the probative value of the extrinsic evidence was not outweighed by unfair prejudice. The extrinsic act evidence was not only similar to the charged scheme in its objectives, but explained the events immediately preceding the formation of the charged conspiracy and the reason the scheme evolved as it did.⁴

The district court did not abuse its discretion in admitting the challenged 404(b) evidence.

III

Barrington also contends that the district court erred in preventing him from cross-examining Jacquette on a pending state burglary charge. A district court's decision limiting cross-examination is likewise reviewed for abuse of discretion. *United States v. Tokars*, 95 F.3d 1520, 1531 (11th Cir. 1996).

The district court disallowed cross-examination into Jacquette's pending state burglary charge because it was unrelated to the case, had not been reduced to a conviction for purposes of Rule 609, and there was no basis on which to believe

⁴ At the conclusion of trial, the jury was appropriately instructed on its consideration of similar act (Rule 404 (b)) evidence, pursuant to Eleventh Circuit Pattern Special Instruction 4.

that Jacquette’s testimony would result in a favorable disposition of his burglary charge. Barrington argues that this ruling prevented him from demonstrating that Jacquette was testifying in an attempt to resolve the burglary charge “and his responsibility for a burglary.” Barrington’s argument is unpersuasive.

The Sixth Amendment guarantees a criminal defendant the right to impeach adverse witnesses through cross-examination. *United States v. Arias-Izquierdo*, 449 F.3d 1168, 1178 (11th Cir. 2006). “A defendant is entitled to cross-examine government witnesses as to any possible motivation for lying or bias, including plea agreements.” *United States v. De Parias*, 805 F.2d 1447, 1452 (11th Cir. 1986), *overruled on other grounds by United States v. Kaplan*, 171 F.3d 1351 (11th Cir. 1999)(en banc). Where the witness is a chief government witness, the right to full cross-examination increases in importance. *Arias-Izquierdo*, 449 F.3d at 1178. And the importance of such cross-examination is not dependent on whether or not “some deal in fact exists between the witness and the government.” *United States v. Lankford*, 955 F.2d 1545, 1548 (11th Cir. 1992).

The right to cross-examine is not unlimited, however. A defendant is not entitled to cross-examine “in whatever way, and to whatever extent, the defense might wish,” *see Delaware v. Fensterer*, 474 U.S. 15, 20 (1985)(per curiam), or to conduct unlimited inquiry into the potential bias of a witness, *De Parias*, 805 F.2d

at 1452 (citing *Delaware v. Van Arsdall*, 475 U.S. 673 (1986)). The Sixth Amendment is satisfied so long as a defendant is permitted cross-examination which “exposes the jury to facts sufficient to evaluate the credibility of the witness and enables defense counsel to establish a record from which he properly can argue why the witness is less than reliable.” *United States v. Baptista-Rodriguez*, 17 F.3d 1354, 1371 (11th Cir. 1994) (citing *United States v. Bennett*, 928 F.2d 1548, 1554 (11th Cir. 1991)).

A district court retains wide latitude to impose reasonable limits on cross-examination. *United States v. Williams*, 837 F.2d 1009, 1015 (11th Cir. 1988); *Baptista-Rodriguez*, 17 F.3d at 1370-71. While cross-examination of a key government witness is important and free cross-examination on possible bias and motive is presumptively favored, “the mere fact that defense counsel sought to explore a prosecution witness's bias does not automatically invalidate ‘the court's ability to limit cross-examination.’” *United States v. Orisnord*, 483 F.3d 1169, 1178 (11th Cir. 2007) (quoting *United States v. Lyons*, 403 F.3d 1248, 1256 (11th Cir. 2005)).

“The test for the Confrontation Clause is whether a reasonable jury would have received a significantly different impression of the witness' credibility had counsel pursued the proposed line of cross-examination.” “As long as sufficient information is elicited from the witness from which the jury can adequately assess possible motive or bias, the Sixth Amendment is satisfied.”

Orisnord, 483 F.3d at 1179 (citations omitted).

Cross-examination of Jacquette on his pending state burglary charge would not have presented a significantly different impression of his credibility. On direct examination, Jacquette told the jury he was in jail, charged with battery, violation of probation and contempt of court as a result of a fight he had with Barrington. The jury understood that Jacquette had been indicted as a co-defendant with Barrington, had pleaded guilty and was testifying pursuant to a Plea and Cooperation Agreement with the United States Attorney's Office, in which the government agreed not to file any additional criminal charges against him in exchange for his cooperation. During cross-examination, Jacquette acknowledged that he hoped to receive a sentence below the Guidelines through a substantial assistance motion from the U.S. Attorney's Office pursuant to U.S.S.G. § 5K1.1. From this line of inquiry, a reasonable juror would appreciate that Jacquette was motivated to testify favorably for the government in hopes of receiving a reduced sentence.

Further, Jacquette acknowledged that Barrington had obtained a state-court restraining order against him and that he had knowingly violated the restraining order by fighting with Barrington, resulting in his contempt of court charge. Cross-examination also brought out that Jacquette harbored ill feelings toward

Barrington, and that there had been issues between them which had escalated into arguments and a fight, pitting one against the other as the criminal investigation progressed.

Jacquette explained that when it became clear that criminal charges would be brought against them for the grade changing scheme, he and Barrington argued and had a “falling out” because Barrington told him “since he and I were close, and we were smarter than [Secrease], that he and I should collaborate our stories and place blame on Lawrence, and let Lawrence take the fall for it.” Jacquette explained that a couple of days later, Secrease called him and shared that Barrington had approached him and suggested that “him and Lawrence should make sure that I take the blame.”

In sum, through cross-examination, Barrington’s counsel elicited sufficient information from Jacquette to enable the jury to assess his credibility, including possible motives and personal bias he held against Barrington. Considering that Jacquette was testifying pursuant to a cooperation agreement with the government and hoped to receive a reduced sentence as a result, questioning him about the pending state burglary charge would not have presented a significantly different impression of his credibility to the jury. At most, Jacquette’s unrelated pending state burglary charge was only marginally relevant, particularly since there was no

showing that he had any agreement, understanding, or “deal” with the government to have that charge favorably disposed of. *See Francis v. Dugger*, 908 F.2d 696, 702 (11th Cir. 1990)(per curiam). Accordingly, the district court did not abuse its discretion by preventing cross-examination on his pending state burglary charges.⁵ *See United States v. Farmer*, 923 F.2d 1557, 1567 n.23 (11th Cir. 1991).

IV

Barrington next contends that Count One of the indictment was duplicative in that it charged two distinct statutory conspiracies, resulting in an improper joinder of offenses. He correctly points out that Count One alleged a conspiracy which violated two statutes, sections 371 and 1349 of Title 18 of the United States Code. Barrington contends that the district court erred in failing to require the Government to elect between the two conspiracy statutes and that the jury should have been instructed on the duplicative nature of Count One and the substantive law of 18 U.S.C. § 1349.

Generally, a defendant must object before trial to defects in an indictment and the failure to do so waives any claimed defects. Fed. R. Cr. P. 12(b)(3)(B), (e); *United States v. Ramirez*, 324 F.3d 1225, 1227-28 (11th Cir. 2003)(per curiam). Barrington did not challenge the indictment in the district court or seek to have the

⁵ It necessarily follows that Barrington’s claim of cumulative evidentiary error is without merit.

Government elect under which of the two conspiracy statutes to proceed. Indeed, in his Rule 29 motion for judgment of acquittal on Count One, he confined his argument to alleged evidentiary deficiencies in the charged § 371 conspiracy, never mentioning § 1349 or any of the contentions he now raises.

Barrington concedes that he did not raise these contentions in the district court. Accordingly, he is deemed to have waived them, absent “good cause.” *United States v. Seher*, 562 F.3d 1344, 1359 n.15 (11th Cir. 2009).⁶ See Fed. R. Crim. P. 12(e) (“For good cause, the court may grant relief from this waiver.”). And he has not demonstrated “good cause” to exempt him from application of this waiver rule. *Seher*, 562 F.3d at 1359 n.15 (“Good cause is not shown where the defendant had all the information necessary to bring a Rule 12(b) motion before the date set for pretrial motions, but failed to file it by that date.”).

Nor did Barrington object to the district court’s use of the Eleventh Circuit’s pattern jury instruction on a § 371 conspiracy or request “an instruction on the duplicitous nature of the indictment” as he now urges should have been given. In

⁶ Absent plain error, an issue which was not raised below will not be considered. *Harden v. United States*, 688 F.2d 1025, 1032 (5th Cir. Unit B 1982). There is no plain error here. Notwithstanding that the conspiracy alleged in Count One violated two distinct conspiracy statutes, 18 U.S.C. § 371 and § 1349, the district court, through a jury instruction expressly requested by Barrington, limited Count One to a § 371 violation. Any claimed duplicity was thereby rendered harmless. See *Reno v. United States*, 317 F.2d 499, 502 (5th Cir. 1963) (duplicity not a fatal defect and where charge is limited to a single violation, any possible duplicity is rendered harmless).

fact, defense counsel requested that Eleventh Circuit Pattern Jury Instruction 13.1 (General Conspiracy Charge, 18 U.S.C. § 371) be used.

Barrington's failure to object to the instruction or submit an alternative instruction results in a waiver unless the instructions which were given constitute plain error. Fed. R. Cr. P 30(d); *United States v. Belfast*, 611 F.3d 783, 822 (11th Cir. 2010). Before an error which was not raised below will be rectified, Barrington must establish (1) error, (2) that is plain, and (3) which affected his substantial rights. *United States v. McNair*, 605 F.3d 1152, 1222 (11th Cir. 2010), *cert. denied*, ___ U.S. ___, 131 S.Ct. 1600, 179 L.Ed.2d 499 (2011). If those three conditions are met, we may exercise our discretion to correct the forfeited error if it "seriously affects the fairness, integrity, or public reputation of judicial proceedings." *Id.*

The jury was correctly instructed on the single conspiracy charged in Count One and the two objects of that conspiracy.⁷ Moreover, Barrington agreed to Count One being submitted to the jury as a violation of 18 U.S.C. § 371.⁸ There was no error, much less error giving rise to a likelihood of a miscarriage of justice

⁷ Barrington does not challenge the sufficiency of the evidence supporting the jury's verdict as to each object of the charged conspiracy. *See United States v. Ross*, 131 F.3d 970, 984 (11th Cir. 1997) (multi-object conspiracy will be upheld if the evidence is sufficient to support a conviction of any of the alleged objects).

⁸ The record does not explain why the parties agreed to submit Count One to the jury solely as a § 371 conspiracy.

or error which affected the fairness of the trial.

Finally, Barrington contends that he was prosecuted on a “legally erroneous fraud theory.” Although his argument is not fully developed, he essentially contends that the grades which were changed do not constitute a property interest and therefore the Government’s proof did not establish the requisite financial deprivation under the wire fraud statute, 18 U.S.C. § 1343. He argues that the jury “was permitted to convict the defendant merely on the theory that he sought to obtain grade changes.”

We construe Barrington’s argument as a contention that the jury’s verdict on Count One rests on an insufficient legal theory. *See United States v. Shotts*, 145 F.3d 1289, 1293 n.3 (11th Cir. 1998). Notwithstanding that Barrington waived this contention by failing to raise it in the district court, we have reviewed for plain error. Finding no plain error, we affirm Barrington’s conviction on Count One.

Count One properly alleged a conspiracy with two objects, the commission of a scheme to defraud by wire and computer fraud. *See United States v. Woodard*, 459 F.3d 1078, 1084 (11th Cir. 2006)(per curiam)(single conspiracy with two unlawful objects). The jury expressly found Barrington guilty of conspiring to commit both objects of the charged conspiracy.

The wire fraud statute, 18 U.S.C. § 1343,⁹ like the mail fraud statute, protects property rights, and the “words ‘to defraud’ signify the deprivation of something of value by trick, deceit, chicane or overreaching.” *United States v. Poirier*, 321 F.3d 1024, 1029 (11th Cir. 2003) (quoting *McNally v. United States*, 483 U.S. 350, 358 (1987)). Similarly, the computer fraud statute, 18 U.S.C. § 1030(a)(4), protects “things of value” by prohibiting unauthorized access to protected computers with the intent to defraud.¹⁰

We have no hesitation in concluding that the Government’s theory rested on a legally cognizable theory of conspiracy to defraud by wire and computer, through which the conspirators deprived FAMU of its property interest in tuition. Count One expressly alleged that the changing of student grades from failing to passing “had the effect of awarding the students who had received the ‘F’ grades thousands of dollars in credit hours to which they were not entitled” and that the change in residency of out-of-state students reduced “the total tuition owed by these students

⁹ Section 1343 provides in pertinent part that “[w]hoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire . . . in interstate or foreign commerce, any . . . signals . . . for the purpose of executing such scheme or artifice, shall be fined . . . or imprisoned . . . or both.” 18 U.S.C. § 1343.

¹⁰ Section 1030(a)(4) provides in pertinent part that one who “knowingly and with intent to defraud, accesses a protected computer without authorization . . . and by means of such conduct furthers the intended fraud and obtains anything of value . . .” commits the offense of computer fraud.

to FAMU by thousands of dollars.”

Barrington’s focus on whether a student’s grade constitutes a property interest is far too narrow.¹¹ Although changing grades was the manner in which the scheme was carried out, the “money or property” of which FAMU was deprived was the lost tuition resulting from the unearned hours credited to the students, rather than the actual grades. Moreover, Barrington ignores the demonstrated financial loss FAMU suffered as a result of the companion aspect of the scheme, the reimbursement of tuition to the out-of-state students whose residencies had been changed.

FAMU undeniably has a property right in tuition generated by class hours a student registers for, as well as the higher tuition paid by non-resident students. By changing failing grades to passing grades, the conspirators endeavored to obtain unearned credit hours for students who were not entitled to them. Had their grades not been changed, those students would have had to repeat the failed classes or take equivalent hours, either of which would have generated additional tuition for

¹¹ Notwithstanding, the Government makes a compelling argument that the students’ willingness to pay to have their grades changed from, for example, a “D” to a “B,” indicates that they placed value in higher grades. Although a higher grade may not be quantifiable in financial terms, the University certainly has an intangible property interest in the integrity of its grading system. Moreover, as alleged in the indictment, increased grade point averages resulting from the grade changes made students eligible for financial aid such as scholarships, loans and grants. Others were able to maintain their scholarships because of their improved GPAs. In sum, there is ample evidence that the scheme alleged in Count One deprived FAMU of property or money and “things of value,” independent of an improved grade in and of itself.

FAMU. By changing the residencies of out-of-state students, the conspirators sought to obtain tuition reimbursement for those students, who otherwise would have been required to pay higher, non-resident tuition. The unearned credit hours and reimbursed tuition constitute “money or property” obtained by wire fraud, as well as “things of value” obtained through computer fraud. No plain error is shown.

V

Barrington next contends that the evidence was insufficient to support his convictions on Counts Three, Four and Five for aggravated identity theft. He argues that the passwords the conspirators used to access the Registrar’s computer system belonged to the university and do not constitute personal identity information of the individual university employees.

Although Barrington moved for judgment of acquittal pursuant to Rule 29, he did not move for judgment of acquittal on the aggravated identity theft counts. Accordingly, we review the sufficiency of the evidence supporting these convictions for plain error. *United States v. Olano*, 507 U.S. 725, 732-36, 113 S.Ct. 1770, 123 L.Ed.2d 508 (1993); *United States v. Snipes*, 611 F.3d 855, 867 n.7 (11th Cir. 2010).

There is no plain error. To prove a violation of 18 U.S.C. § 1028A,¹² the evidence must establish “that the defendant: (1) knowingly transferred, possessed, or used; (2) the means of identification of another person; (3) without lawful authority; (4) during and in relation to a felony enumerated in § 1028A(c).” *United States v. Hurtado*, 508 F.3d 603, 607 (11th Cir. 2007)(per curiam)(footnote omitted), *abrogated on other grounds by Flores-Figueroa v. United States*, ___ U.S. ___, 129 S. Ct. 1886, 173 L.Ed.2d 853 (2009). Wire fraud is one of the enumerated felonies in § 1028A(c).

To gain access to the Registrar’s protected grading system, the conspirators targeted specific “higher up” Registrar employees who they knew had access to the system through their individualized usernames and passwords, which the employees changed every thirty days. Secrease identified the targeted employees and explained that the group established “very close relationships” with these individuals so that “they could get access to their computers.”¹³ The keyloggers were installed on the computers of these targeted employees to obtain their

¹² Section 1028A(a)(1), provides in pertinent part that “[w]hoever, during and in relation to any felony violation enumerated in subsection (c), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years.” 18 U.S.C. § 1028A(a)(1).

¹³ The username was the employee’s first name, followed by a dot, then the employee’s last name.

confidential and unique passwords.

Each of the key elements required for a conviction under § 1028A was proven. The Government proved that Barrington, without authority, knowingly used the usernames and passwords of the Registrar employees during and in relation to the wire fraud conspiracy. The conspirators knew that the usernames and passwords were unique to the employees and would enable them to access the protected grading system. Barrington and his co-conspirators targeted them for that very purpose.

The usernames and passwords were sufficient to identify the specific Registrar employees who had authority to access FAMU's protected grading system. By statutory definition, a "means of identification" includes "any name or number" when used in conjunction with any other information "to identify a specific individual." 18 U.S.C. § 1028(d)(7); *United States v. Mitchell*, 518 F.3d 230, 234 (4th Cir. 2008). The "overriding requirement" of the definition is that the means of identification "must be sufficient to identify a specific individual." *Mitchell*, 518 F.3d at 234(internal quotation marks omitted).

Clearly, the usernames and passwords, considered together, constituted a "means of identification" for those specific individuals and Barrington knew that. *Flores-Figueroa*, 129 S. Ct. at 1894 ("We conclude that § 1028A(a)(1) requires the

Government to show that the defendant knew that the means of identification at issue belonged to another person.”). In sum, the evidence was sufficient to support Barrington’s convictions for aggravated identity theft. There is no plain error.

Next, Barrington contends that the district court erred (1) in failing to instruct the jury that the Government must prove that he “knowingly” used a means of identification that he knew “belonged” to another person and (2) failed to instruct the jury on the term “means of identification,” citing *Flores-Figueroa v. United States, supra*. We review for plain error because Barrington did not object to the district court’s instructions. Fed. R. Crim. P. 30(d); *United States v. Belfast, supra*; *United States v. Sanchez*, 269 F.3d 1250, 1280-81 (11th Cir. 2001) (en banc), *cert. denied*, 535 U.S. 942, 122 S. Ct. 1327, 152 L. Ed.2d 234 (2002).¹⁴

The district court instructed the jury that it could find Barrington guilty “only if all of the following facts are proved beyond a reasonable doubt:

- First: That the defendant knowingly possessed a means of identification of another person; and
- Second: That the defendant possessed the means of identification without lawful authority; and
- Third: That the defendant possessed the means of

¹⁴ In fairness to the district court, this case was tried before *Flores-Figueroa v. United States* was decided.

identification during and in relation to a violation of Title 18, United States Code, Section 1343, namely wire fraud.

While the district court did instruct the jury that Barrington must “knowingly” possess a means of identification, the court did not instruct the jury that Barrington must know that the identification belonged to another person or define the term “means of identification.”

However, even assuming there was arguably plain error in the instructions, Barrington has not carried his burden to show his substantial rights were affected. The evidence was overwhelming that Barrington and his co-conspirators knew that the usernames and passwords they surreptitiously obtained were unique to specific employees of the Registrar’s office. Likewise, the evidence demonstrated beyond all reasonable doubt that they knew that the passwords were a means of verifying those employees’ identities and their authority to access the grading system and therefore belonged to the specific employee. Considering the strength of the evidence and the instruction which was given, we find that the failure of the district court to define the term “means of identification” did not affect Barrington’s substantial rights. Nor, in the context of this case, did the absence of an instruction on the knowing use of a means of identification belonging to another person affect his substantial rights.

In this day and age of protected computer access, jurors are well equipped to apply a common sense definition to the term “means of identification” in the context of this case. No reasonable juror would fail to appreciate that the unique passwords of the targeted Registrar employees belonged to them in the sense that they were “sufficient to identify a specific individual.” Any error in the instructions did not adversely affect the outcome of the trial or the substantial rights of Barrington.

VI

Barrington contends that his 84 month sentence was procedurally and substantively unreasonable. Specifically, he argues that the district court (1) erred in calculating his base offense level under U.S.S.G. § 2B1.1(a)(1); (2) infringed on his right against self incrimination during sentencing by inquiring and commenting on his failure to admit guilt; (3) erred in calculating the loss amount under U.S.S.G. § 2B1.1(b)(1)(F) by including the value of fraudulently received academic credit obtained as a result of grade changes; (4) erred in applying enhancements for the use of sophisticated means under U.S.S.G. § 2B1.1(b)(9)(C) and for a leadership role under U.S.S.G. § 3B1.1(c); and (5) erred in finding that he used device-making equipment and produced unauthorized access devices to support the enhancement under U.S.S.G. § 2B1.1(b)(10)(A)(i) and (B)(i). He also

contends that his sentence was unnecessarily harsh and punitive, considering the sentences of his co-conspirators and those who had participated in the conspiracy but were not charged.

After *United States v. Booker*, 543 U.S. 220, 125 S.Ct. 738 (2005), “a sentence may be reviewed for procedural or substantive unreasonableness.” *United States v. Ellisor*, 522 F.3d 1255, 1273 (11th Cir. 2008) (internal quotation marks omitted). We first review for procedural unreasonableness, to

ensure that the district court committed no significant procedural error, such as failing to calculate (or improperly calculating) the Guidelines range, treating the Guidelines as mandatory, failing to consider the § 3553(a) factors, selecting a sentence based on clearly erroneous facts, or failing to adequately explain the chosen sentence—including an explanation for any deviation from the Guidelines range.

United States v. Shaw, 560 F.3d 1230, 1237 (11th Cir.) (internal quotation marks omitted), *cert. denied*, 129 S.Ct. 2847 (2009).

The procedural reasonableness of a sentence is reviewed for abuse of discretion, “but the degree of deference that is due varies with the type of procedural error alleged.” *Ellisor*, 522 F.3d at 1273 n.25. For example, “[a] district court abuses its discretion if it applies an incorrect legal standard, follows improper procedures in making the determination, or makes findings of fact that are clearly erroneous.” *Id.* (internal quotation marks omitted). Therefore, “[w]e

review *de novo* the district court’s interpretation of the Guidelines and its application of the Guidelines to the facts,” and we review the district court’s findings of fact for clear error. *United States v. Campbell*, 491 F.3d 1306, 1315 (11th Cir. 2007) (internal quotation marks omitted). “A factual finding is clearly erroneous when although there is evidence to support it, the reviewing court on the entire evidence is left with the definite and firm conviction that a mistake has been committed.” *Ellisor*, 522 F.3d at 1273 n.25 (internal quotation marks omitted).

Base offense level

Barrington contends that his conviction under 18 U.S.C. § 1349 was unlawful and therefore the district court erred in relying on that conviction to set the base offense level at 7. Barrington did not object to the calculation of his base offense level in the district court. We review sentencing arguments raised for the first time on appeal for plain error. *United States v. Aguillard*, 217 F.3d 1319, 1320 (11th Cir. 2000)(per curiam).

The district court correctly set the Base Offense Level at 7 pursuant to U.S.S.G. § 2B1.1(a)(1), since the substantive offense Barrington was convicted of conspiring to commit, wire fraud, carries a maximum statutory penalty of 20 years.¹⁵ There is no error, much less plain error.

¹⁵ Counts One and Two were grouped pursuant to U.S.S.G. § 3D1.2(b). Pursuant to U.S.S.G. § 2X1.1, the Base Offense Level for conspiracy is the base offense level from the

Infringement on right against self incrimination

Nor do we find plain error in the district court's query to Barrington during sentencing as to whether he maintained that he did nothing wrong. Near the end of the sentencing hearing, after Barrington's allocution, the district court addressed him:

Mr. Barrington, I sat through your trial. As you know, I was the trial judge. I heard all of the testimony, including yours. And I have yet to hear you say you did wrong. Do you still maintain that you did nothing wrong?

Through counsel, Barrington declined to respond. Counsel explained that if Barrington had not made a showing of remorse, "it's because of my advice, not that it's not coming from him, Your Honor." Barrington did not object under the Fifth Amendment to the district court's question. Accordingly, we review for plain error. *Aguillard*, 217 F.3d at 1320.

Barrington contends that the district court's question infringed upon his Fifth Amendment privilege against self-incrimination. Since Barrington cites *Mitchell v. United States*, 526 U.S. 314, 119 S.Ct. 1307, 143 L.Ed. 2d 424 (1999), we construe his contention to be that the district court impermissibly drew an adverse inference from Barrington's refusal to answer the question and considered that inference in determining the appropriate sentence. *See Mitchell*, 526 U.S. at 328-330

Guidelines for the substantive offense.

(determining, in cocaine conspiracy case where the defendant pled guilty, no negative factual inference may be drawn from a defendant's silence during sentencing with respect to the extent of her participation in the cocaine offense and the amount of cocaine attributable to the defendant).¹⁶

The privilege against self-incrimination applies in a sentencing hearing, and any effort to compel a defendant to testify against his will during sentencing “clearly would contravene the Fifth Amendment.” *Estelle v. Smith*, 451 U.S. 454, 463, 101 S. Ct. 1866, 1873, 68 L. Ed. 359 (1981). And when a defendant shows some sign of remorse but exercises constitutional or statutory rights to remain silent, “the sentencing judge may *not* balance the exercise of those rights against the defendant's expression of remorse to determine whether the ‘acceptance’ [of responsibility] is adequate.” *United States v. Rodriguez*, 959 F.2d 193, 197 (11th Cir. 1992)(per curiam)(determining, in a cocaine conspiracy case, that the district court erred in denying the defendant a reduction in the offense level calculations for acceptance of responsibility based on consideration of defendant’s intention to appeal verdict and refusal to admit guilt in open court). *Mitchell and Rodriguez*,

¹⁶ *But cf. Mitchell*, 526 U.S. at 330 (“Whether silence bears upon the determination of a lack of remorse, or upon acceptance of responsibility for purposes of the downward adjustment provided in § 3E1.1 of the United States Sentencing Guidelines (1998), is a separate question. It is not before us, and we express no view on it.”); *United States v. Henry*, 883 F.2d 1010, 1011-12 (11th Cir. 1989)(per curiam)(conditioning sentence reductions on a defendant's acceptance of responsibility does not violate the Fifth Amendment because such reductions likely will be unavailable to defendants who choose to exercise their Fifth Amendment rights).

however, are factually different because they involve specific Guidelines calculations and other matters, and did not directly address whether the defendant's silence, after some allocution, can bear generally upon a lack of remorse.¹⁷ We need not address that question because the alleged error did not affect Barrington's substantial rights in any event.

While Barrington did not expressly address his involvement in the offense when he allocuted, Barrington certainly attempted to portray himself in a favorable light, alluding to what he had learned from his experience in custody, his attempts to assist other prisoners in attaining their GEDs, and his plan to leave prison a better person. Conspicuously absent from his allocution was any acknowledgment of the offenses for which he had been convicted, or any semblance of remorse. That, coupled with Barrington's trial testimony, apparently prompted the district court to pose the challenged query.

We acknowledge that the district court's question ("Do you still maintain that you did nothing wrong?") and subsequent observation that Barrington had not accepted responsibility might otherwise suggest that it engaged in an impermissible balancing of Barrington's lack of acceptance of responsibility against his exercise of his Fifth Amendment rights. Considered in the proper

¹⁷ Barrington allocuted to some extent. There is no indication that the defendants in *Mitchell* or *Rodriquez* did the same.

context, however, the question and comment, even if error, did not affect Barrington's substantial rights.

In allocuting, Barrington offered nothing by way of remorse, apologizing only to his mother. And it was undisputed that Barrington did not qualify for a downward adjustment for acceptance of responsibility under § 3E1.1 of the Guidelines. During his trial testimony, despite overwhelming evidence against him, Barrington maintained that he had done nothing wrong.

Barrington's trial testimony impacted his sentence in two ways. First, the district court found that Barrington's trial testimony was "materially false" and imposed a two-level enhancement for obstruction of justice pursuant to U.S.S.G. § 3C1.1.¹⁸ Second, contrasting the evidence of good character Barrington presented at sentencing with his lack of acceptance of responsibility during the trial, the district court noted the overwhelming evidence of guilt "displayed an arrogance and contempt for the law."

It is apparent that the district court's question, considered in light of the overwhelming evidence and Barrington's demeanor at trial, was simply an attempt to determine whether Barrington, having had time to reflect, was the least bit

¹⁸ The district court found that Barrington's attempt to conceal from law enforcement the laptop computer used to make the grade changes also supported the obstruction of justice enhancement.

remorseful. He was not.

Further, Barrington's failure to accept responsibility was an appropriate consideration in the determination of his sentence. *Rodriquez*, 959 F.2d at 197 (“The sentencing court is justified in considering the defendant's conduct prior to, during, and after the trial to determine if the defendant has shown any remorse through his actions or statements.”). His lack of remorse, coupled with his false trial testimony, obstructive conduct during the investigation, and what the district court described as his “arrogance and contempt for the law,” certainly justified the sentence imposed, which we note was at the low-end of the Guidelines range.

Finally, Barrington's contention that the district court drew an adverse inference from his silence is entirely speculative. Nothing in the district court's comments evinced an intent to impose a more severe sentence based on Barrington's failure to respond to the district court's question.¹⁹ Barrington merely assumes that the district court relied on an adverse inference in view of the perceived harshness of his sentence. However, his low-end Guidelines sentence belies any such inference having been drawn by the district court. We find no plain error which affected Barrington's substantial rights.

¹⁹ *Compare Thomas v. United States*, 368 F.2d 941, 945 n.10 (5th Cir. 1966) (district court abused its discretion in threatening the defendant with a longer sentence if he did not “come clean and make a clean breast of this thing for once and for all”).

Calculation of financial loss

The district court's determination of loss is reviewed for clear error. *United States v. Bonilla*, 579 F.3d 1233, 1239 (11th Cir. 2009); *United States v. Manoocher Nosrati-Shamloo*, 255 F.3d 1290, 1291 (11th Cir. 2001) (per curiam). And we review the district court's interpretation of the Sentencing Guidelines *de novo*. *United States v. Jordi*, 418 F.3d 1212, 1214 (11th Cir. 2005).

The Guidelines do not require a precise determination of loss. *United States v. Cabrera*, 172 F.3d 1287, 1292 (11th Cir. 1999). “A sentencing court need only make a reasonable estimate of the loss, given the available information.” *United States v. Lee*, 427 F.3d 881, 893 (11th Cir. 2005). Nevertheless, a sentencing judge may not speculate about the existence of a fact that would result in a higher sentence, and the government must support its loss calculation with “reliable and specific evidence.” *Cabrera*, 172 F.3d at 1292(internal quotation marks omitted).

The Guidelines provide that “loss is the greater of actual loss or intended loss.” U.S.S.G. § 2B1.1. cmt. n. 3(A). “Intended loss” is the pecuniary harm that was intended to result from the offense. *Id.*, at cmt. n. 3(A)(ii). The Guidelines acknowledge that a sentencing judge is in a unique position to assess the evidence and estimate the loss and therefore “the court’s loss determination is entitled to appropriate deference.” *Id.* at cmt. n. 3(C). And the Guidelines allow

consideration of the fair market value or replacement cost of the lost property. *Id.* at cmt. n. 3 (C)(i).

Barrington contends that the district court erred in calculating financial loss based on the value of changed grades. The only aspect of intended loss Barrington challenges is the loss attributed to courses in which failing grades were changed to passing grades. He argues that there was no evidence that FAMU either lost or gained money as a result of failing grades being changed to passing grades and the district court's calculation of loss was therefore speculative. Barrington's contentions are unpersuasive, and we find no clear error in the district court's loss calculation.

The Guidelines acknowledge the difficulty in accurately calculating the amount of loss caused by fraud and therefore require only a reasonable estimate of loss. *United States v. Miller*, 188 F.3d 1312, 1317 (11th Cir. 1999)(per curiam); U.S.S.G. § 2B1.1, cmt. n. 3(C). Upon review of the record, we find that the district court's estimate of loss was reasonable.

The district court correctly noted that the Guidelines "allow[] the Court to consider the revenue that would have been generated, as well as the fair market value and replacement cost." It found that passing grades were assigned "to students who did not earn them, and these grades could not have been obtained by

students without retaking the classes.” Further, it found that the “value of the grade change is the cost for retaking the class, which is the figure that has been used to calculate the loss amount.” This finding was based on reliable, specific evidence.

The district court calculated intended loss at \$ 141,830.42, noting that the loss amount was a “conservative and reasonable estimate of the value of the grades.”²⁰ Of that amount, \$ 87,579.52 represented lost tuition for changes from out-of-state to in-state student residencies and \$ 54,250.90 represented 319 credit hours lost for 119 courses for which grades had been changed from failing to passing or had been awarded for classes never taken or from which students had withdrawn.²¹ The loss for each credit hour was determined based on whether the student would have paid in-state or out-of-state tuition.

The district court reasonably concluded that a fraudulent grade represented an academic credit which had a calculable monetary value. The value of the credit hours fraudulently received by the students could be accurately calculated, and the district court’s calculation of loss based on the value of those credit hours was a

²⁰ According to the Florida Department of Law Enforcement (“FDLE”) forensic examination, 650 grades had been changed, and 124 of those were changed from failing to passing grades, resulting in more than \$ 137,000 in lost revenue for FAMU. That amount included, however, the lost tuition resulting from the changed student residencies.

²¹ The loss amount did not include an amount for passing grades which had been changed to higher grades.

reasonable estimate based on the evidence. Testimony established that grades were changed to enhance students' GPAs and qualify them for the next step in their respective academic progressions, including graduate school. Estimating intended loss for those credit hours was hardly speculative, since the students would have had to retake the failed course and pay tuition for the credit hours in order to accomplish their academic goals.²²

In sum, we find that the district court's findings were not clearly erroneous and its determination of intended loss under U.S.S.G. § 2B1.1 was a correct application of the Guidelines.

Sophisticated means enhancement

Barrington next challenges the two-level enhancement for use of sophisticated means. A district court's finding that sophisticated means were used is a finding of fact reviewed for clear error. *United States v. Barakat*, 130 F.3d 1448, 1456-57 (11th Cir.1997). After careful review, we affirm.

The Guidelines provide for a two-level enhancement if an offense involves "sophisticated means." U.S.S.G. § 2B1.1(b)(9)(C). The commentary to § 2B1.1(b)(9)(C) instructs that "'sophisticated means' means especially complex or

²² This logical result was explained by FDLE Special Agent Edward Waters during trial, who calculated FAMU's lost revenue from the scheme.

especially intricate offense conduct pertaining to the execution or concealment of an offense.” *Id.* at cmt. n.8 (B). Each action by a defendant need not be sophisticated in order to support this enhancement. It is sufficient if the totality of the scheme was sophisticated. *See United States v. Finck*, 407 F.3d 908, 915 (8th Cir. 2005) (“Repetitive and coordinated conduct, though no one step is particularly complicated, can be a sophisticated scheme.”).

The district court found that Barrington “used sophisticated means in the execution and attempted concealment of the offense.” Referring to the evidence, the judge noted that after the conspirators failed to obtain the unique Registrar employee passwords by simply watching employees log in to the system, they installed keyloggers on Registrar computers “using stealthy means and personal contacts to do so.” When passwords were changed, the conspirators surreptitiously gained after-hours access to the Registrar computers, installed keyloggers and retrieved the new passwords. When the investigation began and passwords were changed back by the University, the conspirators installed keyloggers again.

As the district court found, “[e]ach of these attempts involved a great deal of planning and inside information,” and “[o]nce the passwords were obtained, the defendants had to learn how to negotiate the FAMU computer system” and “logged on on multiple occasions to practice and learn.” The district court noted that when

the investigation was underway, “the defendants changed random grades in an effort to throw off the investigation, or throw it off track,” and the execution of the scheme and the attempted concealment “involved more than minimal planning and was sophisticated.”

The district court’s findings were supported by the evidence and therefore are not clearly erroneous. The evidence established that Barrington and his co-conspirators repeatedly accessed FAMU’s protected computer grading system using log-in information retrieved through the keyloggers. The hacking involved multiple, repetitive and coordinated steps to deceive and exploit FAMU’s protected system. Even if each step in the scheme was not necessarily sophisticated, suffice it to say that the scheme as a whole used sophisticated means to obtain the unique usernames and passwords and access the Registrar’s protected computer system. *See Campbell*, 491 F.3d at 1315-16.

On this record, we discern no clear error in the district court's factual findings. Barrington’s fraud scheme involved sophisticated means, considering that it involved repetitive and coordinated activities by numerous individuals who used sophisticated technology to perpetrate and attempt to conceal the scheme. The two level enhancement for use of sophisticated means was a correct application of the Guidelines under the circumstances.

Leadership role enhancement

Barrington also challenges his two-level leadership-role enhancement under U.S.S.G. § 3B1.1 (c). He contends that the scheme consisted of a “group of students conducting a loosely coordinated college grades offense,” without a “hierarchy among the college students, who neither worked for each other nor acted as persons subject to the orders of others.” Barrington seemingly ignores the evidence from which the district court made its findings in support of this enhancement.

“A defendant’s role as an organizer or leader is a factual finding that we review for clear error to determine if the enhancement under § 3B1.1 was applied appropriately.” *United States v. Ramirez*, 426 F.3d 1344, 1355 (11th Cir. 2005)(per curiam); *United States v. DeVaron*, 175 F.3d 930, 937 (11th Cir. 1999) (*en banc*). The leadership-role enhancement applies if “the defendant was an organizer, leader, manager, or supervisor in any criminal activity” U.S.S.G. § 3B1.1(c). The defendant does not have to be the sole leader of the conspiracy for the enhancement to apply, and the decision of the district court on this issue is entitled to deference on appeal. *Ramirez*, 426 F.3d at 1355.

The district court articulated several findings in support of the leadership-role enhancement, including that Barrington “led the scheme to change grades by first using paper grade change forms to change his own grades, his sister’s grades,

Christopher Jacquette’s grades and the grades of his fraternity brothers,” and “[w]hen that plan did not work, [he] developed another plan to change grades by accessing the FAMU computer system” and “solicited his co-defendants and others to help;” that Barrington organized a meeting at his residence “and outlined the plan to reinstall keyloggers on the Registrar’s computers, change back the corrected grades and change other grades to throw the investigation off”; that Barrington convinced Jacquette to continue with the grade changing after Jacquette expressed reluctance to continue; and that most of the grade changes were “made from the defendant’s laptop computer.”

We find no error in these findings, much less clear error. Application of the leadership-role enhancement pursuant to § 3B1.1(c) was correct, as demonstrated by the district court’s summary of its findings and justification: “. . . because the defendant initiated the scheme, solicited others to help, and was a driving force behind the attempt to throw off the investigation and continue making grade changes.”

Enhancement for device-making equipment and production of access devices

Barrington’s next challenge is directed to the two-level enhancement for use of “device-making equipment” (keyloggers) and the production of unauthorized access devices (usernames and passwords) under U.S.S.G. § 2B1.1(b)(10). This section authorizes a two-level enhancement if the offense involved (A) “the

possession or use of any (i) device-making equipment . . . ” or (B) “the production or trafficking of any (i) unauthorized access device”

Section 2B1.1(b)(10)(A) applies to an offense involving “the possession or use of any (i) device-making equipment” For purposes of § 2B1.1(b)(10), “‘Device-making equipment’ has the meaning given that term in 18 U.S.C. 1029(e)(6); and (ii) includes (I) any hardware or software that has been configured as described in 18 U.S.C. 1029(a)(9); and (II) a scanning receiver referred to in 18 U.S.C. 1029(a)(8).” U.S.S.G. § 2B1.1 cmt. n.9(A). “‘Scanning receiver’ has the meaning given that term in 18 U.S.C. 1029(e)(8).” *Id.*

“Device-making equipment” is defined to include “any equipment, mechanism, or impression designed or primarily used for making an access device” 18 U.S.C. § 1029(e)(6). “Scanning receiver” is defined as “a device or apparatus that can be used to intercept a wire or electronic communication in violation of chapter 119 [the Federal Wiretap Act, 18 U.S.C. §§ 2510-2522] or to intercept an electronic serial number, mobile identification number, or other identifier of any telecommunications service, equipment, or instrument.” 18 U.S.C. § 1029(e)(8).

Section 2B1.1(b)(10)(B) applies to an offense involving “the production or trafficking of any (i) unauthorized access device” U.S.S.G. § 2B1.1(10)(B). “‘Production’ includes manufacture, design, alteration, authentication, duplication,

or assembly.” *Id.* at cmt. n.9(A). “Unauthorized access device” means “any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud.” 18 U.S.C. § 1029(e)(3); *see also* U.S.S.G. § 2B1.1 cmt. n.9(A) (“‘Unauthorized access device’ has the meaning given that term in 18 U.S.C. 1029(e)(3).”).

For purposes of both the statutory definition of “device-making equipment” and the text of U.S.S.G § 2B1.1(b)(10)(B), an “access device” means “any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument).” 18 U.S.C. § 1029(e)(1).²³

Barrington objected to the Presentence Investigation Report on the ground that “use of key logger software . . . does not satisfy the definition of an apparatus for intercepting the ‘communication’ of identification data.” (Dkt. 140 at 4).

²³ In view of the plain language of this definition and the legislative history of the statute containing it, we have broadly construed the definition of access device to include “innovative means that parties use to gain unauthorized information to engage in fraudulent activities.” *United States v. Dabbs*, 134 F.3d 1071, 1081 (11th Cir. 1998); *see also United States v. Sepulveda*, 115 F.3d 882, 887 n.10 (11th Cir. 1997).

Similarly, Appellant now contends that the district court erred in treating the keylogger software as equivalent to a scanning receiver. Without citing any authority, he also argues that the enhancement in § 2B1.1(b)(10)(A) applies only where the defendant employs an apparatus that remotely intercepts “the ‘communication’ of identification data.”

Appellant did not contend below and does not now contend that the usernames and passwords obtained through use of the keylogger were not a “means of account access” within the meaning of 18 U.S.C. § 1029(e)(1). As explained during trial by FAMU’s Network Infrastructure manager, a keylogger is a device, either hardware-or software-based, that captures “everything a user does, including keystrokes typed or entered on the computer.” He explained that data captured by a keylogger can be retrieved through automatic email, which transmits the keystrokes to a remote email address without the knowledge of the user.

Further, Special Agent Ed Waters described the forensic examination of the Registrar computers and Barrington’s laptop. Agent Waters confirmed that the keyloggers installed on the Registrar computers had captured the usernames and passwords typed into the Registrar computers and that the data had been stored in keylogger logs. The keylogger was configured to send the data to two email addresses associated with Barrington and his co-conspirators, and the keylogger logs reflected that the data had been transmitted to those email addresses.

The explanations of these witnesses support the district court’s finding that the keyloggers used by Barrington and his co-conspirators constituted device-making equipment. The keyloggers captured, stored and were configured to transmit the username and password of an authorized user, and were therefore designed to capture and transmit, and thereby “make” the access device which enabled the conspirators to access identifiable student accounts.²⁴

The username and password combinations could be used to access FAMU’s protected computer system and the students’ accounts to obtain credit hours for classes either failed or not taken and to obtain partial refunds of tuition payments. As discussed, those credits are unquestionably things of value.

Additionally, the conspirators obtained the usernames and passwords with intent to defraud FAMU, thereby rendering them “unauthorized access devices” as defined in 18 U.S.C. § 1029(e)(3) (“any access device that is . . . obtained with intent to defraud.”).

In sum, the record evidence sufficiently supports a finding that keyloggers constitute device-making equipment as defined in 18 U.S.C. § 1029(e)(6).

However, the district court apparently based its conclusion that the keylogger

²⁴ We have suggested in *dictum* that the definition of access device in 18 U.S.C. § 1029(e)(1) should not be extended beyond “devices which access an individual account,” such as a credit card, because, to find otherwise, “would ‘turn § 1029 into a general theft statute applicable whenever a company can document a loss through fraud.’” *United States v. Morris*, 81 F.3d 131, 134 (11th Cir. 1996) (quoting *United States v. Brady*, 13 F.3d 334, 340 (10th Cir. 1993)).

software constituted device-making equipment on the finding that the keylogger software constituted a “scanning receiver.” *See* Dkt. 169 at 46 (“I find that the keylogger software that defendants installed constitutes a scanning receiver and *therefore* meets the definition of device making equipment.”) (emphasis added). We do not believe this finding is adequately supported by the record.

“Scanning receiver” is defined to include any “device or apparatus that can be used to intercept a wire or electronic communication in violation of [the Wiretap Act]” 18 U.S.C. § 1029(e)(8). The Wiretap Act provides criminal and civil sanctions for the unlawful interception of electronic communications. *See id.* §§ 2511(1), 2520. “Intercept” means “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” *Id.* § 2510(4). With exceptions not relevant here, “electronic communication” is defined as “any *transfer* of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce” *Id.* § 2510(12) (emphasis added).

We have held that, to violate the Wiretap Act, an interception of electronic communications must occur contemporaneously with their transmission. *United States v. Steiger*, 318 F.3d 1039, 1048-49 (11th Cir. 2003). Accordingly, use of a

keylogger will not violate the Wiretap Act if the signal or information captured from the keystrokes is not at that time being transmitted beyond the computer on which the keylogger is installed (or being otherwise transmitted by a system that affects interstate commerce).²⁵

Conceivably, the keylogger software at issue here could be used to contemporaneously capture information or signals being transmitted beyond the user's computer. If so, this would bring the keylogger software within the definition of a scanning receiver as "a device or apparatus that *can* be used to intercept a wire or electronic communication in violation of [the Wiretap Act]." 18 U.S.C. § 1029(e)(8) (emphasis added). However, the Government points to no evidence in the record showing that the keylogger at issue here had that capacity and we have found none.

Arguably, the district court's inadequately supported characterization of the keylogger software as a scanning receiver was merely an aspect of a more fundamental finding that the keylogger software constituted device-making equipment, which is fully supported by the record. We need not decide the point because the two-level enhancement was independently supported under U.S.S.G.

²⁵ Cf. *United States v. Scarfo*, 180 F. Supp. 2d 572, 582 & n.5 (D.N.J. 2001) (keylogger configured to record a keystroke only if all the computer's communications ports were inactive did not entail interception of a communication); *United States v. Ropp*, 347 F. Supp. 2d 831, 837-38 (C.D. Cal. 2004) (Wiretap Act's definition of electronic communications applies only to data that is in fact being transmitted beyond a local computer by a system that affects interstate commerce).

§ 2B1.1(10)(B).²⁶

Appellant contends that “viewing or recording of personal identification data” does not constitute “production” of such data within the meaning of U.S.S.G. § 2B1.1(10)(B). That is, Appellant contends that the conspirators did not “produce” an access device within the meaning of the Guideline by acquiring the Registrar employees’ passwords and usernames because those passwords and usernames already existed.

Appellant is mistaken. The contention that a preexisting means of account access cannot be “produced” is contradicted by the plain language of the Guideline application note, which defines the term “production” to include “duplication” or “assembly” of preexisting items. *See* U.S.S.G. § 2B1.1 cmt. n.9(A) (“‘Production’ includes manufacture, design, alteration, authentication, duplication, or assembly.”). The capture, storage, and transmittal of the Registrar employees’ usernames and passwords was at least a duplication or assembly of the usernames and passwords. That the usernames and passwords already existed when they were duplicated or assembled does not matter.

²⁶ *See Williams v. United States*, 503 U.S. 193, 203 (1992) (stating that misapplication of the Guideline requires remand “unless the reviewing court concludes, on the record as a whole, that the error was harmless, *i.e.*, that the error did not affect the district court's selection of the sentence imposed.”); *United States v. Kendrick*, 22 F.3d 1066, 1068 (11th Cir. 1994) (recognizing that if a Guidelines error “did not affect the district court's selection of the sentence imposed” the sentence should be affirmed)(quoting *United States v. Jones*, 1 F.3d 1167, 1171 (11th Cir. 1993)).

The district court expressly found that the “defendants produced unauthorized access devices when they retrieved the passwords and user names from the data on the keyloggers.” That finding was not clear error and the application of the two-level enhancement for production of an unauthorized access device under U.S.S.G. § 2B1.1(10)(B) was proper.

In conclusion, the district court did not abuse its discretion with respect to any of Barrington’s claimed procedural errors. None of the issues have merit and his sentence was procedurally reasonable.

Substantive Reasonableness

Having concluded that the district court’s sentence was procedurally sound, we turn to Barrington’s challenge to the substantive reasonableness of his sentence. *Gall v. United States*, 552 U.S. 38, 51, 128 S. Ct. 586, 597 (2007). The substantive reasonableness of a sentence is reviewed for abuse of discretion, based on the totality of the circumstances. *United States v. Livesay*, 525 F.3d 1081, 1091 (11th Cir. 2008).

In arriving at a substantively reasonable sentence, the district court must consider the sentencing factors listed in 18 U.S.C. § 3553(a), including (1) the nature and circumstances of the offense and the history and characteristics of the defendant; (2) the need to reflect the seriousness of the offense, to promote respect

for the law, and to provide just punishment for the offense; (3) the need for deterrence; (4) the need to protect the public; (5) the need to provide the defendant with needed educational or vocational training or medical care; (6) the kinds of sentences available; (7) the Sentencing Guidelines range; (8) pertinent policy statements of the Sentencing Commission; (9) the need to avoid unwanted sentencing disparities; and (10) the need to provide restitution to victims. *United States v. Talley*, 431 F.3d 784, 786 (11th Cir. 2005)(per curiam)(citing 18 U.S.C. § 3553(a)).

Although the district court must consider the § 3553(a) factors, it need not “state on the record that it has explicitly considered each of the § 3553(a) factors or . . . discuss each of [them].” *United States v. Scott*, 426 F.3d 1324, 1329 (11th Cir. 2005). It is sufficient for the district court to explicitly acknowledge that it considered the parties’ arguments at sentencing which were based on the sentencing factors, and that it considered the factors in § 3553(a). *Id.* The weight given to each factor in § 3553(a) is “a matter committed to the sound discretion of the district court.” *United States v. Clay*, 483 F.3d 739, 743 (11th Cir. 2007) (internal quotation marks omitted). “The fact that [we] might reasonably have concluded that a different sentence was appropriate is insufficient to justify reversal of the district court.” *Gall*, 552 U.S. at 51, 128 S.Ct at 597.

We review for reasonableness in light of the § 3553(a) factors, including whether the sentence “fail[ed] to achieve the purposes of sentencing as stated in section 3553(a).” *Id.* Barrington bears the burden of showing that his sentence was unreasonable. *Talley*, 431 F.3d at 788; *United States v. Tome*, 611 F.3d 1371, 1378 (11th Cir.), *cert. denied*, 131 S.Ct. 674 (2010). He has not met his burden.

In announcing its sentence, the district court explicitly considered the § 3553(a) factors, expressly noting the “facts and circumstances surrounding this particular case,” and the seriousness of the offense. Barrington’s sentence was at the low end of the advisory Guidelines, suggesting that the district court considered Barrington’s mitigation arguments. While a range of reasonable sentences is available to the district court, ordinarily a sentence within the advisory Guidelines range is reasonable. *United States v. Chavez*, 584 F.3d 1354, 1365 (11th Cir. 2009), *cert. denied*, 131 S.Ct. 436 (2010).

Upon consideration of the parties’ briefs and a review of the record, we conclude, based on the totality of the circumstances, that Barrington’s low-end Guideline range sentence was consistent with the § 3553(a) factors and therefore reasonable. *United States v. Pugh*, 515 F.3d 1179, 1190 (11th Cir. 2008).

Accordingly, we affirm.

AFFIRMED.