IRM PROCEDURAL UPDATE

DATE: 11/27/2013

NUMBER: PGLD-10-1113-1689

SUBJECT: Handling Taxpayer Inquiries Regarding Data Loss Letters

AFFECTED IRM(s)/SUBSECTION(s): 10.5.4

CHANGE(s):

IRM 10.5.4.4.5.1 - Reorganized to improve clarity and flow and updated instructions to transfer individuals who call on other than the telephone number provided in Letter 4281C to Application 92161 (or 92162 for individuals needing assistance in Spanish) to resolve a discrepancy between IRM 10.5.4 and the Telephone Transfer Guide.

1. The contact telephone number provided in Letter 4281C, *IM Breach Notification Letter*, is 1-866-225-2009. The Identity Protection Specialized Unit (IPSU) supports this dedicated number and is trained to respond to IRS data loss questions and questions regarding Letter 4281C.
2. The IPSU answers general incident related inquiries regarding the data loss and prepares an Inquiry Referral Form (Form 4442) if the caller requests specific information regarding the incident that the IPSU is unable to answer. The Form 4442 is directed to the Incident Management office in Philadelphia for resolution.
3. In some instances, individuals who receive Letter 4281C may call an IRS telephone number other than the number provided in the letter (1-866-225-2009). If an IRS phone assistor other than an assistor in the IPSU receives a call from an individual in response to Letter 4281C, or the individual asks to speak to the employee whose number appears on Letter 4281C (0847999999), transfer the call to extension 92161 (for callers needing assistance in Spanish, use extension 92162).
4. Correspondence received in response to Letter 4281C, or addressed to employee 0847999999, must be forwarded to the IPSU at the following address: IRS, Attn: IPSU, PO Box 9039, Andover, MA, 01810–9039. If the correspondence appears to be time sensitive, fax it to the Image Control Team (ICT) in Andover at (855)807-5720. The IPSU can provide further assistance regarding the data loss incident and information to protect the taxpayer's personal data.

Exhibit 10.5.4-1 – Added a Header Row to the exhibit.

Term	Definition

Access	The ability or opportunity to gain knowledge of personally identifiable information.
Breach	The loss of control, disclosure, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.
Data Loss (Breach) Notification	The process of notifying potentially impacted individuals following the evaluation of a PII data loss incident which results in a high risk of harm to these individuals. Also known as PII data loss incident notification.
Data Loss Incident Risk Assessment	A risk assessment conducted on an IRS incurred data loss, theft, breach, or disclosure incident. The risk assessment includes factors that must be considered, specifically the context of the incident and the data that was disclosed. Example - An IRS employee in the field loses a taxpayer case file assigned to him. It contained PII data such as name, address, SSN, and other tax data. It is not known if the loss of the PII data will lead to identity theft. The IRS conducts a risk assessment and examines key factors to determine if notification should be given to the taxpayer.
Federal Information Processing Standards (FIPS)	A set of standards that describe document processing, encryption algorithms and other information technology standards for use within non-military government agencies and by government contractors and vendors who work with the agencies.
Federal Information Processing Standards (FIPS) Publications	Publications issued by NIST after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Reform Act of 1996 (Public Law 104-106) and the Federal Information Security Management Act of 2002 (Public Law 107-347).
Federal Trade Commission (FTC)	An independent agency of the United States government, established in 1914 by the Federal Trade Commission Act, with the principal mission of promoting "consumer protection" and the elimination and prevention of what regulators perceive to be "anti-competitive" business practices.
Harm	Includes any of the following effects of a breach of confidentiality, integrity, availability, or fiduciary responsibility:

	a) Potential for blackmail;
	b) Disclosure of private facts;
	c) Mental pain and emotional distress;
	d) Potential for secondary uses of the information that could result in fear or uncertainty, or unwarranted exposure leading to humiliation or loss of self-esteem;
	e) Identity theft; or
	f) Financial loss.
Identity Theft	A fraud that is committed or attempted using a person's identifying information without authority.
Incident Management	The process of managing incidents involving the loss, theft, breach or disclosure of data. This term can also be used to refer to the Office within Privacy, Governmental Liaison and Disclosure responsible for the process of managing incidents involving the loss, theft, breach or disclosure of data by the IRS.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency.
Loss	Any event where an item is misplaced and/or neither the official owner nor the intended recipient has possession of the item in the expected time frame. A loss may involve an IRS-owned physical asset such as a laptop, blackberry, cell phone, and/or other portable media, or electronic or hard copy data that may contain Sensitive But Unclassified (SBU) data or Personally Identifiable Information (PII) such as paper or electronic taxpayer records, personnel records, or other identifying data, or a combination of a physical asset and electronic and/or hard copy data.
National Institute of Standards and Technology (NIST)	A non-regulatory federal agency within the U.S. Department of Commerce that develops and promotes measurement, standards, and technology.
The Office of Management and Budget (OMB)	OMB assists the President in overseeing the preparation of the Federal budget and evaluates the effectiveness of agency programs, policies, and procedures, and works to make sure that agency reports, rules, testimony, and proposed legislation are consistent with the President's Budget and with Administration policies. In addition, OMB oversees and coordinates the Administration's regulatory, procurement, financial management, information

	technology, and information management policies.
Personally Identifiable Information (PII)	Personally Identifiable Information is any information that, by itself or in combination with other information, may be used to uniquely identify an individual. See OMB 07-16. and the PGLD web page PII - What is personally identifiable information? for additional information.
PII Incident	An actual or suspected loss of control, disclosure, unauthorized disclosure, unauthorized acquisition of, or unauthorized access to PII. PII incidents include situations where persons other than authorized users may or do have access to PII for an unauthorized purpose. This applies to PII maintained in electronic or hard copy format.
PII Incident Notification	See **Data Loss (Breach) Notification**.
PII Incident Management Working Group (IMWG)	A decision making body chaired by the Deputy Director, Incident Management. Membership consists of senior management and key technical experts from all key business and functional unit stakeholders. Policy roles include: a) Reviewing Incident Management Program policy analyses and recommendations, b) Providing further analysis, data collection and support material for the Privacy and Information Protection Advisory Committee (PIP AC) decision making, and c) Providing recommendations to the AC for final decision making. Operational roles include: a) Reviewing Incident Management case risk analyses and recommendations, b) Providing further analysis, data collection and support material for AC decision making, c) Approving low-risk case decisions, and d) Providing medium and high-risk case recommendations for victim notification to the AC for final decision making.
Privacy and Information Protection Advisory Committee (PIP AC)	A committee established to oversee the Identity Protection Program and Incident Management Program activities, specifically the development of Servicewide identity theft and PII data loss policies and procedures, development and execution of Identity Protection and Incident Management Program office procedures, and the study and execution of identity theft outreach, victim assistance and prevention initiatives.
Risk	The level of impact on agency operations (including mission, functions, image, or reputation), agency

	assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
Risk Assessment	The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security and privacy controls that would mitigate this impact.
Safeguard	Any action, device, procedure, technique, or other measure that reduces a system's vulnerability to a threat.
Sensitive But Unclassified Information	Any information that requires protection due to the risk and magnitude of loss or harm to the IRS or the privacy to which individuals are entitled under 5 U.S.C. § 552a (the Privacy Act), which could result from inadvertent or deliberate disclosure, alteration, or destruction.
Theft	An asset, electronic or hardcopy, thought or known to have been taken without permission from the person who is responsible for the asset.
Unauthorized Access	The willful unauthorized access and/or inspection of tax returns and return information.
Unauthorized Disclosure	An unauthorized and unlawful release of information to an individual who is not authorized to receive the information.
Unreasonable Delay	A delay in notification following the discovery of a data breach beyond that which is necessary to determine the scope of the breach while considering the needs of law enforcement and national security, and, if applicable, to restore the reasonable integrity of the computerized data system compromised. This means if a breach is discovered and all the information necessary to determine the scope of the breach is gathered within 30 days, it is unreasonable to wait until the 45th day to notify the individuals whose information was breached.